Patent Application Transmittal

(only for new nonprovisional applications under 37 C.F.R. 1.53(b))

Correspondence Address:
FROMMER LAWRENCE & HAUG LLP
745 FIFTH AVENUE
NEW YORK, NEW YORK 10151
TEL: (212) 588-0800
FAX: (212) 588-0500

Date: April 7, 1999
Attorney Docket No.: 450100-3689.1

ASSISTANT COMMISSIONER FOR PATENTS
Box Patent Application
Washington, D.C. 20231

Sir:

With reference to the filing in the United States Patent and Trademark Office of an application for patent in the name(s) of: Ryuji Ishiguro and Masafumi Minami

entitled: ENCRYPTING METHOD AND APPARATUS, RECORDING METHOD, DECRYPTING METHOD AND APPARATUS, AND RECORDING MEDIUM

X Continuing Application

X Continuation ___ Divisional ___ Continuation-in-Part (CIP)
of prior application Serial No. 08/721,310, filed October 15, 1996.

[Note: If priority under 35 U.S.C. 120 involves a series of respectively copending applications, then in this amendment identify each and its relationship to its immediate predecessor.]

X The prior application is assigned of record to Sony Corporation.

__ This is an application of a small entity under 37 CFR 1.9(f) and the amounts shown in parentheses below have been employed in calculating the fee:
__ Small Entity Verified Statement(s) is (are) enclosed.
___ Small Entity Verified Statement(s) filed in prior application, status still proper and desired

The following are enclosed:

X Specification (54 pages)
X 14 Sheet(s) of Drawings
X 37 Claim(s) (including 15 independent claim(s))
___ This application contains a multiple dependent claim

X Our check for $2,002.00, calculated on the basis of the claims as amended by any enclosed preliminary amendment as follows:

Basic Fee, $760.00 ($380.00)	$ 760.00
Number of Claims in excess of 20 at $18.00 ($9.00) each:	306.00
Number of Independent Claims in excess of 3 at $78.00 ($39.00) each:	936.00
Multiple Dependent Claim Fee at $260.00 ($130.00)	
Total Filing Fee	$2,002.00

___ Assignment Recording Fee $40.00 . . . . . .

___ This application is being filed within the month following the expiration of the term originally set therefor in the prior application. This is a petition to request a -month extension of time. A check covering the cost of the petition is enclosed.

Patent Application Transmittal

(only for new nonprovisional applications under 37 C.F.R. 1.53(b))

450100-3689.1

_X_ Oath or Declaration and Power of Attorney
___ New ___ signed ___ unsigned
_X_ Copy from a prior application (37 C.F.R. 1.63(d))

Deletion of Inventors

___ Signed Statement attached deleting inventor(s) named in the prior application (37 C.F.R. 1.63(d)(2) and 1.33(b))

Power of Attorney or Correspondence Address Change

_X_ Power of attorney and/or correspondence address was changed during prosecution of the prior application. The new power of attorney is to **William S. Frommer, Reg. No. 25,506**. The new correspondence address is indicated above.

_X_ Incorporation by Reference (for continuation or divisional application) The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

_X_ A Preliminary Amendment is enclosed.
(Claims added by this amendment have been properly numbered consecutively beginning with the number next following the highest numbered original claim in the prior application.)

_X_ Cancel in this application original claims 2-59 of the prior application before calculating the filing fee. (At least one original independent claim must be retained for filing purposes.)

__ New formal drawings are enclosed.

_X_ Certified copy of each foreign priority application on which the claim for priority under 35 U.S.C. 119 is based was filed in prior U.S. application Serial No. 08/721,310, filed October 15, 1996. A list of said foreign priority application(s) is (are) provided below. Acknowledgement thereof is requested.

Application No.	Filed	In
07-267262	October 16, 1995	Japan

Please charge any additional fees required for the filing of this application or credit any overpayment to Deposit Account No. 50-0320.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicant(s)

By: _____
William S. Frommer
Reg. No. 25,506

PATENT
450100-3689.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Ryuji Ishiguro et al.
Serial No.	:	Continuation of Serial No. 08/721,310
For	:	ENCRYPTING METHOD AND APPARATUS, RECORDING METHOD, DECRYPTING METHOD AND APPARATUS, AND RECORDING MEDIUM
Filed	:	Herewith
Examiner	:	P. M. Laufer
Art Unit	:	2766

745 Fifth Avenue
New York, NY 10151

EXPRESS MAIL

Mailing Label Number: EM009638395US

Date of Deposit: April 7, 1999

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington, DC 20231.

Charles Jacobs
(Typed or printed name of person mailing paper or fee)

Charles Jacobs
(Signature of person mailing paper or fee)

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Prior to issuance of the first Office Action in the above-referenced patent application, please amend the application as follows:

IN THE SPECIFICATION

Please substitute the enclosed revised specification. The amendments are noted in the "mark up" copy of the specification submitted herewith.

Page 1, before line 1, add the following:

--This is a continuation of co-pending Application Serial No. 08/721,310 having a filing date of October 15, 1996.--

IN THE CLAIMS

Please cancel claims 1-59.

Add the following new claims:

--60. A method of encrypting information to generate encrypted data and recording the encrypted data onto a recording medium, comprising the steps of:

generating an encryption key based on key data which is recorded to predetermined regions on the same surface as the encrypted data and determined from said recording medium yet is not part of said encrypted data; and

encrypting the information based on said encryption key.--

--61. An apparatus for encrypting information to generate encrypted data and recording the encrypted data onto a recording medium, comprising:

means for generating an encryption key based on key data which is recorded to predetermined regions on the same surface as the encrypted data and determined from said recording medium yet is not part of said encrypted data; and

means for encrypting the information based on said encryption key.--

--62. A method of recording information on a recording medium, comprising the steps of:

receiving said information in the form of encrypted data which represents said information, said encrypted data having been generated through the use of an encryption key, wherein said encryption key is based on key data which is recorded to predetermined regions on the same surface as the encrypted data and determined from said recording medium yet is not part of said encrypted data; and

recording said received encrypted data on said recording medium.--

--63. The method according to claim 62, wherein said key data includes the wobbling frequency of a wobbled pre-groove and/or wobbled land portion of said recording medium.--

--64. The method according to claim 63, further comprising the steps of generating a file indicative of one or more positions on said recording medium and recording said file on said recording medium; wherein the frequency of at least one wobbled pre-groove and/or at least one wobbled land portion located at said positions is used as said key data.--

--65. A method of encrypting information to generate encrypted data and recording the encrypted data onto a recording medium, comprising the steps of:

generating an encryption key based on key data which is recorded to predetermined regions on the same surface as the encrypted data and determined from said recording medium yet is not part of said encrypted data; and

encrypting the information based on said encryption key;

wherein said key data is random data which has been inserted in-between said encrypted data at predetermined positions.--

--66. The method according to claim 65, further comprising the steps of:

generating a file indicative of a predetermined portion of said random data; and

recording said file on said recording medium.--

--67. The method according to claim 65, wherein said random data is recorded on said recording medium as a normal file according to the ISO9660 standard.--

--68. The method according to claim 65, wherein said random data is recorded on said recording medium as an interleaved file.--

--69. The method according to claim 65, wherein said random data is recorded on said recording medium as a multi extent file.--

--70. The method according to claim 65, wherein said random data is recorded in a pre gap area of a file according to the ISO9660 standard.--

--71. The method according to claim 65, wherein said random data is recorded in a system area of a file according to the ISO9660 standard.--

--72. The method according to claim 65, wherein said random data is recorded in an application area of a primary volume descriptor of a file according to the ISO9660 standard.--

--73. The method according to claim 65, wherein said random data is recorded on a surface of said recording medium.--

--74. The method according to claim 65, wherein said random data is data selected from a predetermined portion of a random file generated by a pseudo random generator.--

--75. The method according to claim 74, further comprising the steps of:

generating a file indicative of said predetermined portion of said random file; and

recording said file and said random file on said recording medium.--

--76. An apparatus for encrypting information to generate encrypted data and recording the encrypted data onto a recording medium, comprising:

means for generating an encryption key based on key data which is recorded to predetermined regions on the same surface as the encrypted data and determined from said recording medium yet is not part of said encrypted data; and

means for encrypting the information based on said encryption key;

wherein said key data is random data which has been inserted in-between said encrypted data at predetermined positions.--

--77. The apparatus according to claim 76, further comprising:

means for generating a file indicative of a predetermined portion of said random data, and recording said file on said recording medium.--

--78. The method according to claim 76, wherein said random data is recorded on said recording medium as a normal file according to the ISO9660 standard.--

--79. A method of recording information on a recording medium, comprising the steps of:

receiving said information in the form of encrypted data which represents said information, said encrypted data having been generated through the use of an encryption key, wherein said encryption key is based on random data which has been recorded to predetermined regions on the same surface as the encrypted data and inserted in-between said encrypted data yet is not part of said encrypted data; and

recording said received encrypted data on said recording medium.--

--80. The method according to claim 79, wherein a file of said encrypted data and a file indicative of a predetermined portion of said random data are recorded on said recording medium.--

--81. The method according to claim 79, wherein said random data is data selected from a predetermined portion of a random file generated by a pseudo random generator.--

--82. The method according to claim 81, further comprising the steps of:

generating a file indicative of said predetermined portion of said random file; and

recording said file and said random file on said recording medium.--

--83. The method according to claim 79, wherein said random data is recorded on said recording medium as a normal file according to the ISO9660 standard.--

--84. A method of recording information on a recording medium, comprising the steps of:

receiving said information in the form of encrypted data which represents said information, said encrypted data having been generated through the use of an encryption key, wherein said encryption key is based on data which has been recorded to the surface of said recording medium and which is not part of said encrypted data; and

recording said received encrypted data on said recording medium.--

--85. A method of decrypting encrypted data that has been recorded on a recording medium, comprising the steps of:

reproducing a first file from said recording medium, said first file containing said encrypted data, wherein said encrypted data has been encrypted by an encryption key and said encryption key is based on random data which has been recorded to predetermined regions on

the same surface as the encrypted data and inserted in-between said encrypted data yet is not part of said encrypted data;

reproducing a second file containing data indicative of a predetermined portion of said random data which has been recorded to and inserted into said encrypted data;

detecting random data within said encrypted data according to said second file;

generating a decryption key based on said detected random data; and

decrypting said encrypted data of said reproduced first file by using said decryption key.--

--86. A method of decrypting encrypted data that has been recorded on a recording medium, comprising the steps of:

reproducing a first file from said recording medium, said first file which was recorded to predetermined regions on the same surface as the encrypted data on said recording medium and containing said encrypted data, wherein said encrypted data has been encrypted by an encryption key and said encryption key is based on random data selected from a predetermined portion of a random file, said random file being generated by a pseudo random data generator;

reproducing said random file from said recording medium

reproducing a second file from said recording medium, said second file containing data indicative of said predetermined portion of said random file;

generating a decryption key based on said random data as obtained from said random file according to said second file; and

decrypting said encrypted data of said reproduced first file by using said decryption key.--

--87. An apparatus for decrypting encrypted data that has been recorded on a recording medium, comprising:

means for reproducing a first file from said recording medium, said first file containing said encrypted data, wherein said encrypted data has been encrypted by an encryption key and said encryption key is based on random data which has been recorded on predetermined regions on the same surface as the encrypted data on said recording medium and inserted in-between said encrypted data yet is not part of said encrypted data; and for reproducing a second file containing data indicative of a predetermined portion of said random data which has been inserted into said encrypted data;

means for detecting random data within said encrypted data according to said second file;

means for generating a decryption key based on said detected random data; and

means for decrypting said encrypted data of said reproduced first file by using said decryption key.--

--88. An apparatus for decrypting encrypted data that has been recorded on a recording medium, comprising:

means for reproducing a first file from said recording medium, said first file containing said encrypted data, wherein said encrypted data has been encrypted by an encryption key and said encryption key is based on random data recorded on said recording medium on predetermined regions on the same surface as the encrypted data and selected from a predetermined portion of a random file, said random file being generated by a pseudo random data generator; for reproducing said random file from said recording medium; and for

reproducing a second file from said recording medium, said second file containing data indicative of said predetermined portion of said random file;

means for generating a decryption key based on said random data as obtained from said random file according to said second file; and

means for decrypting said encrypted data of said reproduced first file by using said decryption key.--

--89. A recording medium comprising:

a storage area for storing data;

encrypted data and random data recorded therein for use in the encryption of data, said encrypted data having been encrypted according to an encryption key which is based on said random data which was recorded on predetermined regions on the same surface as the encrypted data on said storage area.--

--90. The recording medium according to claim 89, further comprising data indicative of a predetermined portion of said random data.--

--91. A recording medium comprising:

a storage area for storing data; and

encrypted data stored therein for use in the encryption of data, said encrypted data having been encrypted according to an encryption key which is based on the wobbling frequency of one or more predetermined portions of said recording medium.--

--92. The recording medium according to claim 91, further comprising data indicative of said one or more predetermined portions of said recording medium.--

--93. A recording medium comprising:

a storage area for storing data; and

encrypted data and random data stored therein, said encrypted data having been encrypted according to an encryption key which is based on said random data, and wherein said random data is selected from a predetermined portion of a random file which is generated by a pseudo random generator and was recorded on predetermined regions on the same surface as the encrypted data on said storage area.--

--94. The recording medium according to claim 93, further comprising stored therein data indicative of the portion of said random file corresponding to said random data.--

--95. A recording medium comprising:

a storage area for storing data; and

encrypted data stored therein, said encrypted data having been encrypted by using a second encryption key, wherein said second encryption key is generated based on a first encryption and a third encryption key, said first encryption key which being based on key data which is recorded on predetermined regions on the same surface as the encrypted data and determined from said recording medium yet is not part of said encrypted data, and said third encryption key being independent of said first encryption key.--

REMARKS

In light of the above amendatory matter and remarks to follow, reconsideration and allowance of this application are requested. This Amendment is responsive to the Final Office Action in the parent case of August 6, 1998.

The Examiner's remarks in the last Official Action in the parent application have been carefully considered. In response, Applicants' representative believes that all of the claims in this application are allowable.

The Applicants have made numerous amendments to the specification. The amendments are indicated in the "mark-up" copy of the specification submitted herewith, and they include the revisions specified by the Examiner in an Office Action in the parent case. The amendments are made for purposes of clarification and they do not add any new matter to the application.

The drawings are corrected as requested in an Office Action in the parent case in accordance with the Request for Approval of Drawing Change submitted herewith.

In this Amendment, claims 60-95 have been added which are the same as claims 60, 63, 66-88, 96, 98, 102, 103 and 107-113 in the parent case.

In the Final Office Action of the parent case claims 69-87, 96 and 102 (which are now claims 65-83, 85 and 87) were rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Claims 65, 76, 79, 85 and 87 have been rewritten to overcome the rejections. Therefore Applicants request that the rejection of these claims based upon 35 U.S.C. §112, second paragraph, be withdrawn.

Claims 107-113 (now claims 89-95) were rejected under 35 U.S.C. §112, first paragraph because the specification does not reasonable provide enablement for the "single means" claims. Claims 107-113 (now claims 89-95) were rejected under 35 U.S.C. §101 because they are non-statutory. These claims have been rewritten to overcome the rejections. Therefore Applicants request that the rejection of these claims based upon 35 U.S.C. §101, be withdrawn.

Claims 60, 63, 66-69, 80-88, 96, 98, 102, 103, 107, 108, 111 and 112 were rejected under 35 U.S.C. §102(b) as being anticipated by Narasimhalu et al. ('718). Claims 63, 66, 83, 84, 87, 88, 102, 103, 107 and 108 35 U.S.C. §102(e) as being anticipated by Kikinis ('947). Claims 63, 66, 88 and 107 are rejected under 35 U.S.C. §102(e) as being anticipated by

Kondo ('773). Claims 70-79 are rejected under 35 U.S.C. §103 as being unpatentable over Narasimhalu et al. ('718). In response, the rejections are traversed for the following reasons.

Applicants' invention as recited in rewritten independent claim 60 requires generating an encryption key based on data which is "recorded to predetermined regions on the same surface as the encrypted data and determined from said recording medium yet is not part of said encrypted data." Applicants' claims therefore require that the data on which the encryption is based be recorded on the surface of the disk. Also, the data must be recorded on the same surface of the disk.

Narashimhalu et al. merely discloses using selected defects in the disk surface and not data recorded on the disk to encrypt information on the disk. Kondo merely discloses to record encrypting information on the edge of the disk. Kikinis merely discloses selectively obliterating the readability of bits in addressable sectors to encode data. None of the cited references teach or suggest the above features of the present invention. Therefore, withdrawal of the rejections are respectfully requested. If the Examiner does not withdraw the rejections, the Examiner is requested to identify those elements of the references which support his rejections.

Independent claims 61-62, 65, 76, 79, 84-89, 91, 93 and 95 include limitations corresponding to independent claim 60, and will not be analyzed to avoid repeating the above analysis. It is apparent, however, that claims 61-62, 65, 76, 79, 84-89, 91, 93 and 95 are distinguishable over the prior art for the same reasons as claim 1 discussed hereinabove.

Due to their dependency, claims 66-75, 77-78, 80-83, 90, 92 and 95 incorporate all of the limitations of the independent claims including the above-discussed features. It is apparent, therefore, that dependent claims 66-75, 77-78, 80-83, 90, 92 and 95 are, at a minimum, distinguishable over the prior art for the same reasons as Applicants' independent claims.

In light of the above, Applicants' representative traverses the Examiner's rejections and respectfully submits that the references, alone or in combination do not teach or suggest all of the features of the present invention, as claimed. In view of the foregoing amendments and remarks, it is believed that all of the claims now in this application are patentable over the prior art. Early and favorable consideration thereof is solicited. On the basis of the above amendments and remarks, reconsideration and allowance of this application are respectfully requested.

The above statements concerning the disclosures in the cited references represent the present opinion of Applicants' representative and, in the event that the Examiner disagrees, Applicants' representative respectfully requests the Examiner specifically indicate those portions of the respective references providing the basis for a contrary view.

Applicants' representative agrees with the Examiner that the prior art made of record and not relied upon is not as relevant to the claimed invention as are the references upon which the Examiner has relied.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicant's representative at the telephone number listed below.

The Commissioner is hereby authorized to charge any insufficient fees or credit any overpayment associated with the above-identified application to Deposit Account 50-0320.

Respectfully submitted,
FROMMER LAWRENCE & HAUG LLP

By: 
William S. Frommer
Reg. No. 25,506
(212) 588-0800

PATENT
450100-3689

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

TITLE: ENCRYPTING METHOD AND APPARATUS, RECORDING METHOD, DECRYPTING METHOD AND APPARATUS, AND RECORDING MEDIUM

INVENTORS: Ryuji Ishiguro
Masafumi Minami

William S. Frommer
Registration No. 25,506
Curtis, Morris & Safford, P.C.
530 Fifth Avenue
New York, New York 10036
(212) 840-3333

ENCRYPTING METHOD AND APPARATUS, RECORDING METHOD, DECRYPTING METHOD AND APPARATUS, AND RECORDING MEDIUM

BACKGROUND OF THE INVENTION

1. Field of the Invention:

The present invention relates to encrypting method and apparatus, decrypting method and apparatus, and a recording medium in which information encrypted by an encrypting method or an encrypting apparatus is recorded, and, for example, encrypting method and apparatus, decrypting method and apparatus, and a recording medium suitable for use in a system in which information such as video signals, audio signals, data signals or the like is encrypted, the encrypted information is recorded on a recording medium, and the encrypted information is decrypted.

2. Description of the Related Art:

When information is encrypted and then recorded on a predetermined recording medium, information is encrypted by using a predetermined encryption key and the encrypted information is recorded on the recording medium. The encrypted information is decrypted by using a decryption key for decrypting the encrypted information recorded on the recording medium.

A cryptosystem employing a key (an encryption key) includes two cryptosystems; a common-key cryptographic scheme and a public-key cryptosystem. In the common-key cryptosystem, a key (encryption key) used upon encryption is the same as a key

(decryption key) used upon decryption. For example, of the common-key cryptosystems, a data encryption standard (DES) system is frequently employed. On the other hand, in the public-key cryptosystem, an encryption key and a decryption key are different from each other. In this public-key cryptosystem, the encryption key is opened to the public, but the decryption key is kept secret. In general, such encryption method and decryption method are known.

An encryption method is disclosed in Japanese patent publication No. 60007/1990. According to the method, an encryption key is generated based on a data forming a file to be recorded on a recording medium. Information is encrypted by using the encryption key, and the encrypted information is recorded on the recording medium. The file is reproduced from the recording medium, and a decryption key is generated based on data forming the file. Then, the encrypted information is decrypted by using the generated decryption key.

However, when such encryption method and decryption method are employed, the file used for generating the encryption key is recorded on one portion (sequent regions) of the recording medium, which may allow the file to be duplicated with comparative ease.

SUMMARY OF THE INVENTION

In view of such aspect, it is an object of the present invention to provide encryption method and apparatus, a recording method, and decryption method and apparatus which allows strong copy protect to be effected on the information

recorded on a recording medium, and a recording medium where information encrypted by the encrypting apparatus is recorded.

According to a first aspect of the present invention, when information to be recorded is encrypted by using an encryption key, an encryption key based on inherent information inherent in a recording medium is generated. The information to be recorded on the recording medium is encrypted based on the encryption key. The inherent information inherent in the recording medium is a specific information on a disk.

According to a second aspect of the present invention, an encrypting apparatus for encrypting information to be recorded by using an encryption key includes a means for generating an encryption key based on inherent information inherent in a recording medium, and a means for encrypting the information to be recorded on the recording medium based on the encryption key. The inherent information inherent in the recording medium is a specific information on a disk.

According to a third aspect of the present invention, when information obtained by encrypting information to be recorded by using an encryption key is recorded on a recording medium, an encrypted information is received based on an encryption key generated based on inherent information inherent in a recording medium. The received encrypted information is recorded on a recording medium. The inherent information inherent in the recording medium is a specific information on a disk.

According to a fourth aspect of the present

invention, when an encrypted information recorded on a recording medium is decrypted, there are reproduced from a recording medium a first file storing information encrypted by using an encryption key generated based on a random data to be inserted into a predetermined portion of the encrypted information to be recorded on a recording medium and a second file storing data indicative of a predetermined portion of the random data to be inserted into a predetermined portion of the encrypted information. The random data is detected from the encrypted information stored in the reproduced first file based on the data stored in the reproduced second file and indicating the predetermined portion of the random data. A decryption key is generated from the detected random data. The encrypted information of the reproduced first file is decrypted by using the decryption key.

According to a fifth aspect of the present invention, a decrypting apparatus for decrypting an encrypted information recorded on a recording medium includes a means for reproducing from the recording medium a first file storing information encrypted by using an encryption key generated based on a random data to be inserted into a predetermined portion of the encrypted information to be recorded on a recording medium and a second file storing data indicative of a predetermined portion of the random data to be inserted into a predetermined portion of the encrypted information, a means for detecting the random data from the encrypted information stored in the reproduced first file based on the data stored in the reproduced second

file and indicating the predetermined portion of the random data, a means for generating a decryption key from the detected random data, and a means for decrypting the encrypted information of the reproduced first file by using the decryption key.

According to a sixth aspect of the present invention, a recording medium capable of being used in decryption by a decrypting apparatus includes a recorded signal capable of being decrypted by a decrypting apparatus,. The recorded signal includes a first file storing information encrypted by using an encryption key generated based on random data to be inserted into a predetermined portion of an encrypted information.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a first embodiment of the present invention;

FIG. 2 is a diagram showing a logical file format according to ISO9660 standard;

FIG. 3 is a flowchart used to explain an encrypting operation of an encrypting apparatus according to the first embodiment of the present invention;

FIG. 4 is a table showing an example of an arrangement of a digest method file;

FIG. 5 is a diagram used to explain a method of producing a disk digest;

FIG. 6 is a flowchart used to explain a decrypting operation of a decrypting apparatus according to the first

embodiment of the present invention;

FIG. 7 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a second embodiment of the present invention;

FIG. 8 is a flowchart used to explain an encrypting operation of an encrypting apparatus according to the second embodiment of the present invention;

FIG. 9 is a flowchart used to explain a decrypting operation of a decrypting apparatus according to the second embodiment of the present invention;

FIG. 10 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a third embodiment of the present invention;

FIG. 11 is a flowchart used to explain an encrypting operation of an encrypting apparatus according to the third embodiment of the present invention;

FIG. 12 is a flowchart used to explain a decrypting operation of a decrypting apparatus according to the third embodiment of the present invention;

FIG. 13 is a diagram used to explain encrypting and decrypting methods employed by the encrypting and decrypting apparatus according to the third embodiment;

FIG. 14 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to a fourth embodiment of the present invention; and

FIG. 15 is a cross-sectional view showing a disk having an inherent information recorded on its surface.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

An embodiment of the present invention will hereinafter be described with reference to the accompanying drawings. Informations used in this embodiment are video informations, audio informations, text informations and so on. In this embodiment, recording media on which encrypted information to be decrypted is recorded are, for example, disk-like recording media such as digital video disks (DVD), optical disks, magneto-optical disks, magnetic disks such as flexible disks or hard disks, and so on, and tape-like recording media such as magnetic tapes or the like.

These recording media are slave recording media a large number of which are produced by duplication of a master disk, a master magnetic tape or the like. Data (plain text) to be encrypted is data subjected to the scrambling, the shuffling, the encoding according to moving picture experts group (MPEG) system, the encoding according to joint photographic experts group (JPEG) system and so on. In accordance with the data to be encrypted, data (plain text) decrypted from encrypted data is data to be subjected to the de-scrambling, the de-shuffling, the decoding according to the MPEG system, the decoding according to the JPEG system and so on.

FIG. 1 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus according to the first embodiment of the present invention, by way of example.

An encrypting apparatus 1 includes an information

data generating unit 2 which is formed of a reproducing apparatus for reproducing an information data (such as digital video information, digital audio information or the like) from a recording tape and so on on which the information data is recorded. THe data generating unit 2 outputs the reproduced information data (plain text) to an encrypting unit 3. The encrypting unit 3 encrypts the information data output from the information data generating unit 2 and outputs an encrypted information data (cryptogram) to a recording unit 7 which will be described later on.

The encrypting apparatus also includes an inherent information generating unit 5 which outputs information inherent in a recording medium to the recording unit 7. A random data (random number data) or the like is employed as the information inherent in the recording medium. The random data is recorded by the recording unit 7 on a predetermined region of the recording medium such as a disk or the like as a normal file as shown in FIG. 2. Indeed, since the random data is the normal file, the random data can be copied. But, when this file is copied to the recording medium such as a hard disk or the like, as shown in FIG. 2, a position (allocation) of this file is changed, which prevents the same information as that of an original disk from being obtained.

FIG. 2 is a diagram showing a logical file format according to the ISO9660 standard. As shown in FIG. 2, sectors 0 to 149 are set as a pre gap area where data may or may not be recorded. Sectors 150 to 165 are set as a system area where a

copyright information is stored, for example. Subsequent sectors 166 to n-1 (were n is a variable number and a predetermined integer value) are set as volume descriptors where management informations are stored.

The volume descriptors include a primary volume descriptor where a table of directories (path table) and so on are stored. Sector n and succeeding sectors are user-accessible areas where predetermined files are stored. Each of the sectors is formed of 2 kbytes, and an offset is used to indicate a position therein.

As shown in FIG. 2, for example, the random data can be recorded as an interleaved file. Moreover, the random data can be recorded as a multi extent file. The interleaved file is a file of the random data recorded on a plurality of discontinuous portions in a predetermined area. The multi extent file is a file of the random data which are recorded on a plurality of discontinuous areas as one file.

When the random data is recorded as the interleaved file or the multi extent file, the random data can be recorded on dispersed positions, which makes it more difficult to match the position of the random data recorded on the read-only disk with the position of the random data obtained by copying the random data from the read-only disk.

Moreover, it is possible to record the random data on the pre gap area (00:00:00:00 to 00:00:02:00) or on the system area (00:00:02:00 to 00:00:02:16) according to the ISO9660 standard. When the random data is recorded on either of the

above areas, the recorded random data cannot be accessed as the normal file, which makes it difficult to copy the random data.

Moreover, it is possible to record the random data on an application area with its offset within the range from 884th byte to 1395th byte of the primary volume descriptor of the volume descriptor according to the ISO9660 standard. Since this application area stores a header information of the files according to the ISO9660 standard, the random data recorded on the area cannot be accessed as the normal file, which makes it difficult to copy the random data stored therein.

The random data is finally recorded on a master disk 12 as shown in FIG. 1.

The encrypting apparatus 1 includes a file forming unit 6 for forming a file (digest method file) indicative of a predetermined portion of an encrypted information data. Specifically, the file forming unit 6 designates the random data from a predetermined byte number to another predetermined byte number in the same sector or over different sectors of the random data recorded on the master disk 12 with being inserted in the above encrypted information data. Then, the file forming unit 6 forms a file (digest method file) formed of one or plural pairs of sector numbers and offsets (byte number in a sector). The file indicative of a predetermined portion of the information data (the digest method file) is inserted into an predetermined area in the encrypted information data and finally recorded on the master disk 12.

The encrypting apparatus 1 includes the recording

unit 7 for recording on a hard disk 8 the random data supplied from the inherent information generating unit 5, the digest method file supplied from the file forming unit 6, and the encrypted information data supplied from the encrypting unit 3. The encrypting apparatus 1 includes a reproducing unit 9 formed of a magnetic head, an amplifier and so on. The reproducing unit 9 reads out the random data from the hard disk 8 based on the digest method file recorded on the hard disk 8 and supplies the read random data to the encryption key generating unit 4. The reproducing unit 9 also reads out the encrypted information data and supplies the encrypted information data together with the random data and the digest method file to a formatting unit 10.

The formatting unit 10 formats the encrypted information data and the digest method file supplied from the reproducing unit 9 to produce a pre-master image. The formatting unit 10 supplies the pre-master image to the recording unit 7. At this time, as described above, the formatting unit 10 can format the random data as the normal file according to the ISO9660 standard, and, as described above, can format the data as the interleaved file or the multi extent file. The recording unit 7 records the pre-master image on the hard disk 8. The encrypting apparatus 1 includes a recording unit 11 formed of an optical head, an amplifier and so on. The recording unit 11 records the pre-master image reproduced from the hard disk 8 by the reproducing unit 9 on the master disk 12. A disk producing apparatus 13 employs the master disk 12 as an

original disk to reproduce a large number od disks 15 (slave disks).

A decrypting apparatus 14 includes a reproducing unit 16, a decrypting unit 17, a decryption-key generating unit 18, and an output terminal 19. The reproducing unit 16 reproduces the disk 15. The decryption-key generating unit 18 generates a decryption key based on a reproduced signal supplied from the reproducing unit 16, and outputs the decryption key to the decrypting unit 17 which will be described later on. The decrypting unit 17 decrypts the reproduced signal supplied from the reproducing unit 16 based on the decryption key supplied from the decryption-key generating unit 18.

An encrypting operation of the encrypting apparatus 1 will be described with reference to FIG. 3 which is a flowchart therefor. In step S1, initially, the inherent information generating unit 5 generates the random data (random-number data) which is a value (encryption key) inherent in a recording medium and supplies the random data to the recording unit 7. In this step, the file forming unit 6 determines from which area of the master disk 12 the random data (random-number data) used for the value (encryption key) inherent in the recording medium is extracted, and then produce a file (digest method file) indicative of one or a plurality of determined areas.

As shown in FIG. 4, for example, the digest method file is formed of a table including a large number of offsets (offset numbers) of n sectors from the sector number 1 to the sector number n (where n is the number of about several tens).

As shown in FIG. 5, the table designates data from a predetermined offset in a sector of the sector number 1 to another predetermined offset therein and data from a predetermined offset in a sector of the sector number 2 to another predetermined offset therein. The digest method file is recorded by the recording unit 7 on the hard disk 8. The random data is also recorded by the recording unit 7 on the hard disk 8.

The processing proceeds to step S2. The reproducing unit 9 reproduces the random data of the digest method file, which is determined in step S1 and recorded on the hard disk 8, from the predetermined offset in the sector of the sector number 1 to another predetermined sector therein and from the predetermined offset in the sector of the sector number 2 to another predetermined offset therein. The reproducing unit 9 then gathers the reproduced random data. The reproducing apparatus 9 supplies these gathered random data to the encryption-key generating unit 4.

In step S3, the encryption-key generating unit 4 subjects the random data supplied from the reproducing unit 9 to a predetermined calculation (e.g., addition) or generates the encryption key (inherent value, disk digest) from the random data itself as shown in FIG. 5. Then, the processing proceeds to step S4. In step S4, the encryption-key generating unit 4 supplies the generated encryption key to the encrypting unit 3. The encrypting unit 3 encrypts the information data supplied from the information data generating unit 2 based on the

supplied encryption key. The encrypting unit 3 supplies the encrypted information data to the recording unit 7. Then, the recording unit 7 records the encrypted information data on the hard disk 8.

Then, the processing proceeds to step S5. the reproducing unit 9 reproduces the encrypted information data, the random data which is to be the information inherent in the recording medium, and the digest method file indicative of the predetermined portion of the encrypted information data which are recorded on the hard disk 8, and supplies them to the formatting unit 10. The formatting unit 10 generates the pre-master image (format signal) from the encrypted information data, the random data which is to be the information inherent in the recording medium, and the digest file method file indicative of the predetermined portion of the encrypted information data all of that are supplied from the reproducing unit 9. At this time, as described above, the formatting unit 10 formats the random data as the normal file according to the ISO9660 standard. Moreover, the formatting unit 10 can format the random data as the interleaved file or the multi extent file to be dispersed.

The formatting unit 10 supplies the produced pre-master image to the recording unit 7. The recording unit 7 temporarily records the pre-master image on the hard disk 8. The reproducing unit 9 reproduces the pre-master image recorded on the hard disk 8 and supplies the reproduced data to the recording unit 11. The recording unit 11 records the reproduced

data supplied from the reproducing unit 9 on the master disk 12. Alternatively, the formatting unit 10 can supply the pre-master image, i.e., the formatting signal directly to the recording unit 11 which records the pre-master image on the master disk 12.

The disk producing apparatus 13 employs the master disk thus produced as an original disk to reproduce a large number of the disks (slave disks such as a DVD, an optical disk, a magneto-optical disk, or the like) 15. When the magnetic tape is employed as the recording medium, a transfer apparatus may be employed to transfer signals recorded on the master magnetic tape to a large number of slave magnetic tapes.

A decrypting operation of the decrypting apparatus 14 will be described with reference to FIG. 6 which is a flowchart therefor. In step S11, the reproducing unit 16 reproduces the signals recorded on the disk 15. The reproducing unit 16 supplies the reproduced signal to the decrypting unit 17 and, when the decryption-key generating unit 18 supplies a gate signal to the reproducing unit 16, also supplies a file of the recorded signal where the random data is stored and the digest method file to the decryption-key generating unit 18.

The processing proceeds to step S12. In step S12, the decryption-key generating unit 18 extracts from the random data supplied from the reproducing unit 16 the random data designated by the digest method file, e.g., the random data from the predetermined offset to another predetermined offset in the sector of the sector number 1 and the random data from the

predetermined offset to another predetermined offset in the sector of the sector number 2, and then gathers the extracted random data.

Then, the processing proceeds to step S13. In step S13, the decryption-key generating unit 18 generates the decryption key corresponding to the original encryption key from the random data gathered in step S12 and subjected to the predetermined calculation (e.g., addition) or from the random data itself. The decryption-key generating unit 18 supplies the generated decryption key to the decrypting unit 17. Then, the processing proceeds to step S14. In step S14, the decrypting unit 17 decrypts the reproduced data supplied from the reproducing unit 16, i.e., the encrypted information data (cryptogram) based on the decryption key supplied from the decryption-key generating unit 18, thus obtaining the original information data (plain text). The decrypting unit 18 outputs the original information data through the output terminal 19.

If the encrypting apparatus 1 records pit strings of the recording signal on the track of the master disk 12 in a wobbled fashion, then the inherent information generating unit 5 may generates a wobbling signal indicative of the wobbling of the pit strings of the recording signal to be recorded on the master disk 12 as the information signal inherent in the recording medium 12. If the information inherent in the disk 15 as the recording medium is a physical information to be formed on the disk 15 and a track on which the recording signal of the master disk 12 is to be recorded is a wobbled pregroove or a

wobbled land portion, the wobbling signal corresponding to the pregroove or the land portion may be generated as the information signal inherent in the recording medium from the inherent information generating unit 5.

The encryption-key generating unit 4 generates an encryption key based on the wobbling signal and supplies the generated encryption key to the encrypting unit 3. The encrypting unit 3 encrypts the information data supplied from the information data generating unit 2 based on the encryption key supplied from the encryption-key generating unit 4.

In this case, the decrypting apparatus 14 is operated as follows. Specifically, the decryption-key generating unit 18 detects a wobbling frequency of the pregroove or the land portion corresponding to the predetermined portion of the recording signal on the disk 15. The decryption-key generating unit 18 generates the decryption key obtained by subjecting the data corresponding to the wobbling frequency to a predetermined calculation or generates the decryption key corresponding to the original encryption key based on the data itself corresponding to the wobbling frequency. The decryption-key generating unit 18 supplies the generated decryption key to the decrypting unit 17. The decrypting unit 17 decrypts the encrypted information data (cryptogram) supplied from the reproducing unit 16 by using the decryption key supplied from the decryption-key generating unit 18, to obtain the original information data (plain text).

As described above, if the information inherent in the recording medium is the physical information to be recorded

on the recording medium, e.g., the wobbled pregroove or the wobbled land portion of the recording medium, then the recording medium may be a disk having a considerable thickness and a comparatively rigid substrate, such as a DVD, an optical disk, a magneto-optical disk, a hard disk or the like.

When the random data is employed as the information inherent in the recording medium and the position where the random data is recorded is managed by the digest method file as described above, it is possible to effect the effective copy protect in the information.

Since the normal file according to the ISO9660 standard is employed, and when the file is duplicated to the recording medium, the file is recorded on a different position of the recording medium, it is impossible to obtain the same information as that of the original disk. Therefore, it is possible to effect the more effective copy protect on the information.

FIG. 7 is a block diagram showing an arrangement of an encrypting apparatus and a decrypting apparatus, to which the encrypting and decrypting method according to the present invention is applied, according to a second embodiment of the present invention. An encrypting apparatus 1 shown in FIG. 7 has a random file forming unit 20 instead of the inherent information generating unit 5 of the encrypting apparatus 1 shown in FIG. 1 and also has a file forming unit 21 for forming a file indicative of a predetermined portion of the random file instead of the file forming unit 6 for forming a file indicative

of the predetermined portion of the encrypted information. Other arrangements and operations of the encrypting and decrypting apparatus 1 and 14 shown in FIG. 7 are similar to those of the encrypting and decrypting apparatus 1, 14 shown in FIG. 1 and hence will not be described.

An operation of the encrypting apparatus 1 shown in FIG. 7 will be described with reference to FIG. 8 which is a flowchart therefor. The random file forming unit 20 includes a pseudo random data generator for generating a random data. In step S21, the random file forming unit 20 produces a random file including a random data of, for example, several kbytes or larger generated by the pseudo random data generator. The random file forming unit 20 supplies the random file, for example, to the recording unit 7. The recording unit 7 records the random file on the hard disk 8.

Then, the processing proceeds to step S22. In step S22, the file forming unit 21 determines from which portions of the random file random-number data (random data) used for obtaining an inherent value (encryption key) is gathered, i.e., determines from which portions of the random data the random data from a predetermined offset number to another offset number or the random data formed of a plurality of predetermined portions is gathered. The file forming unit 21 forms a digest method file indicative of the predetermined portions of these random data and supplies the digest method file to the recording unit 7. The recording unit 7 once records the digest method file on the hard disk 8. Finally, the reproducing unit 9 reads

out the recorded digest method file from the hard disk 8 and supplies the reproduced digest method file to the recording unit 11, and the recording unit 11 records the digest method file on the master disk 12.

Then, the processing proceeds to step S23. In step S23, the reproducing unit 9 gathers the random data, recorded on the hard disk 8, of the one predetermined portion from the predetermined offset address to another predetermined offset address or the random data, recorded on the hard disk 8, of a plurality of predetermined portions, and reproduces them. The reproducing unit 9 supplies the reproduced random data to the encryption-key generating unit 4. The encryption-key generating unit 4 generates the encryption key (inherent value) (disk digest) from the random data itself or the random data subjected to the predetermined calculation.

Then, the processing proceeds to step S24. In step S24, the position where the random file is allocated in the master disk 12 is calculated, i.e., there is calculated an offset value (offset number) of a predetermined sector number obtained when the random file is inserted into the encrypted information data recorded on the hard disk 8 and then recorded on the master disk 12. The calculated offset value is added to the offset number (offset value) designated by the digest method file. Thus, the digest method file is modified.

Then, the processing proceeds to step S25. In step S25, the encryption-key generating unit 4 supplies the generated encryption key (the inherent value) (disk digest) to the

encrypting unit 3. The encrypting unit 3 encrypts the information data supplied from the information data generating unit 2 and supplies the encrypted information data to the recording unit 7. The recording unit 7 records the encrypted information data on the hard disk 8.

Then, the processing proceeds to step S26. In step S26, the reproducing unit 9 reproduces the encrypted information data, the signal indicative of the information inherent in the recording medium, and the digest method file indicative of the predetermined encrypted portion from the hard disk 8 and supplies them to the formatting unit 10. The formatting unit 10 formats the information data, the information signal and the digest method file to produce the pre-master image. In this formatting operation, as described above, the formatting unit 10 can format the random file as the interleaved file or the multi extent file to disperse the random file to the different positions.

The formatting unit 10 supplies the pre-master image to the recording unit 7. The recording unit 7 once records the pre-master image on the hard disk 8. The reproducing unit 9 reproduces the pre-master image recorded on the hard disk 8 and supplies the reproduced pre-master image to the recording unit 11. The recording unit 11 records on the master disk 12 the pre-master image supplied from the reproducing unit 9 or the pre-master image supplied directly from the formatting unit 10.

The disk producing apparatus 13 employs the master disk 12 as the original disk to obtain a large number of the

disks (slave disks) 15 by duplication of the master disk 12.

A decrypting operation of the decrypting apparatus 14 shown in FIG. 7 will be described with reference to FIG. 9 which is a flowchart therefor. In step S31, the reproducing unit 16 reproduces the disk 15 and supplies the reproduced data to the decryption-key generating unit 18. Then, the processing proceeds to step S32. In step S32, the decryption-key generating unit 18 extracts from the reproduced encrypted information data the random data, designated by the digest method file, of a portion from the predetermined offset to another predetermined offset in the sector of the predetermined sector number and of another portion from the predetermined offset to another predetermined offset. The decryption-key generating unit 18 gathers them.

Then, the processing proceeds to step S33. In step S33, the decryption-key generating unit 18 generates the decryption key obtained by subjecting the random data to the predetermined calculation or the decryption key corresponding to the original encryption key based on the random data itself and then supplies the generated decryption key to the decrypting unit 17. Then, the processing proceeds to step S34. In step S34, the decrypting unit 17 decrypts the encrypted information data (cryptogram) supplied from the reproducing unit 16 by using the decryption key supplied from the decryption key supplied from the decryption-key generating unit 18 to obtain the original information data (plain text). The decrypting unit 17 outputs the original information data through the output

terminal 19.

FIG. 10 is a block diagram showing arrangements of an encrypting apparatus and a decrypting apparatus according to a third embodiment of the present invention. An arrangement of the encrypting apparatus 1 shown in FIG. 10 is basically similar to the encrypting apparatus shown in FIG. 1 and hence will not be described.

An encryption method employed by the encrypting apparatus 1 shown in FIG. 10 will be described with reference to FIG. 11 which is a flowchart therefor. In step S41, a distribution key (distribution-key data) to be distributed to a user is properly determined and registered in a memory (e.g., a semiconductor memory) in the encryption-key generating unit 4. The distribution key may be registered in a central processing unit (CPU) (which may include the memory) instead of the memory.

Then, the processing proceeds to step S42. In step S42, similarly to the processing described above with reference to the flowchart of FIG. 3, the encryption-key generating unit 4 gathers the informations inherent in the disk 15 and subjects the informations to a predetermined calculation to generate the disk digest (key). Then, the processing proceeds to step S43. In step S43, the encryption-key generating unit 4 subjects the distribution key determined in step S41 and the disk digest generated in step S42 to a predetermined calculation, e.g., exclusive-ORs the distribution key and the disk digest and sets the calculated result as a work key.

The processing proceeds to step S44. In step S44,

the encryption-key generating unit 4 supplies the work key obtained through the calculation in step S43 to the encrypting unit 3 as the encryption key. The encrypting unit 3 encrypts the information data based on the encryption key and supplies the encrypted information data to the recording unit 7. The recording unit 7 records the encrypted information data on the hard disk 8.

The decrypting apparatus 14 shown in FIG. 10 has a key reading unit 22 and a key medium 23 newly provided in addition to those of the decrypting apparatus 14 shown in FIG. 1. The key medium 23 is arranged such that the above-mentioned distribution key can be distributed. For example, the distribution key may be printed on some suitable object in the form of Arabic numerals, symbols, bar codes, other codes similar to the bar codes or the like. The key medium 23 can be formed of a card or the disk 15 itself.

The key medium 23 may includes a memory, such as a semiconductor memory or the like, storing the distribution key or a CPU or the like including the memory. The key medium 23 including the memory or the CPU may be formed of a card (e.g., an integrated circuit (IC) card) or the like. The key medium 23 may be arranged such that the distribution key is recorded thereon magnetically or optically. Such key medium 23 is to be sold on a market solely or together with a reproducing apparatus for reproducing the disk 15. The key reading unit 22 reads out the distribution key printed on or recorded on the key medium 23.

A decrypting operation of the decrypting apparatus 14 shown in FIG. 10 will be described with reference to FIG. 12 which is a flowchart therefor. In step S51, the key reading unit 22 reads out the distribution key printed on or recorded on the key medium 23 and supplies the distribution key to the decryption-key generating unit 18. Then, the processing proceeds to step S52. In step S52, similarly to the processing decryption processing described with reference to FIG. 6, the decryption-key generating unit 18 gathers the informations inherent in the disk 15 and subjects the informations to a predetermined calculation, thereby obtaining the disk digest (key) corresponding to the original disk digest (key).

Then, the processing proceeds to step S53. In step S53, the decryption-key generating unit 18 subjects the distribution key obtained in step S51 and the disk digest obtained in step S52 to a predetermined calculation, e.g., exclusive-ORs the distribution key and the disk digest, thereby obtaining the work key. Then, the processing proceeds to step S54. In step S54, the decryption-key generating unit 18 supplies the work key obtained in step S53 as the decryption key to the decrypting unit 17. The decrypting key 17 decrypts the encrypted information data supplied from the reproducing unit 16 by using the decryption key supplied from the decryption-key generating unit 18 and then outputs the decrypted information data through the output terminal 19.

FIG. 13 is a diagram used to explain the encryption method and the description method respectively employed in the

encrypting apparatus 1 and the decrypting apparatus 14 shown in FIG. 10. Specifically, the plain text is encrypted based on the distribution key and the disk digest, and the cryptogram obtained by encryption of the plain text is recorded on the disk. The distribution key is supplied to a user through a route other than the disk. The cryptogram read out from the disk is decrypted based on the disk digest obtained by calculation of the distribution key and the data read out from predetermined one or plural areas of the disk. Thus, the decrypted plain text is output.

FIG. 14 is a block diagram showing an encrypting apparatus and a decrypting apparatus according to a fourth embodiment of the present invention.

An encrypting apparatus 1 shown in FIG. 14 has a random file forming unit 20 and a random file forming unit 21 for forming a file indicative of a predetermined portion of the random file both similar to those shown in FIG. 7 instead of the inherent information generating unit 5 and the file forming unit 6 of the encrypting apparatus 1 shown in FIG. 10. The random file forming unit 20 and the file forming unit 21 are operated basically similarly to those described with reference to FIG. 7 and other units are also operated basically similarly to the those described with reference to FIG. 10. Therefore, the operations of the encrypting apparatus 1 and the decrypting apparatus 14 shown in FIG. 14 will not be described. The encrypting apparatus 1 and the decrypting apparatus 14 having such arrangements can carry out the operations of encrypting the

plain text and decrypting the cryptogam obtained by encryption of the plain text by the method shown in FIG. 13.

Even if any of the encrypting apparatus 1 according to the first to fourth embodiments is employed to read the information data (file) from the predetermined recording medium (the disk 15 in this case) and to dub (or copy) the information data on another predetermined medium, then it is impossible to obtain the same data as recorded on the original recording medium from another recording medium because the information data is usually recorded on another recording medium at the positions different from those where the information data is recorded on the original recording medium. Therefore, it is impossible to decrypt the encrypted information data. Alternatively, even if the information data recorded on another recording medium can be decrypted, it is impossible to output the decrypted information data through the output terminal as the digital signals. As a result, employment of the encrypting apparatus and method makes it difficult to copy the information data to another recording medium.

Since the random file is arranged as the interleaved file or the multi extent file and hence recorded on the different and dispersed positions of the recording medium, as described above, it becomes more difficult to match the positions of the random data recorded on the read-only disk with the positions of the random data copied on the hard disk from the read-only disk. Therefore, the illegitimate dubbing (copying) can be suppressed.

In each of the first to fourth embodiments, as shown in FIG. 15, the information inherent in the disk 15 can be recorded by ultraviolet laser or the like on a disk surface, i.e., a surface of the disk substrate 33.

When the information inherent in the disk which is recorded on the surface of the disk substrate 33 is read out, rays of light must be condensed on the surface of the disk substrate 33 by moving an optical head (not shown) in the direction perpendicular to the disk surface ,and further a special reading apparatus and a special reading command (e.g., a command to move the optical head in the direction perpendicular to the disk surface) are required. Therefore, it becomes difficult to read the information thus recorded, and it becomes impossible to easily copy such information.

This arrangement can also be effective in protecting the information from an optical copy or a so-called "peel and copy". The "peel and copy" is to physically copy pits 32 formed on the disk substrate 33 after a protective film 31 is peeled off from the disk substrate 33. Specifically, the information inherent in the disk is recorded or printed on the disk substrate 33, it is possible to protect the information inherent in the disk from the "peel and copy" and the optical copy in which rays of light are irradiated on the pits 32 of the disk substrate 33 and the copy is carried out based on the reflected light or the transmission light.

The apparatus and methods according to the first to fourth embodiments of the present invention can be utilized for

communication such as wire communication (e.g., communication through an electric cable, an optical fiber cable or the like), wireless communication (communication utilizing electric waves, light, sound waves or the like), or the like. In this case, the encrypting apparatus 1 supplies the cryptogram to the decrypting apparatus 14 through the wire communication or the wireless communication.

While the file is formatted in accordance with the ISO9660 standard in the first to fourth embodiment, the present invention is not limited thereto. While the work key is generated by calculating the distribution key and the disk digest in the first to fourth embodiments, the present invention is not limited thereto. The work key may be generated by calculating the distribution key and the wobbling signal.

According to the encrypting apparatus and method of the present invention, since the information inherent in the recording medium is set as the frequency of the predetermined portion of the wobbled pregroove or the wobbled land portion to be formed on the recording medium, it is possible to effect the strong copy protect on the information.

According to the encrypting apparatus and method of the present invention, since the information inherent in the recording medium is set as the random data to be inserted into the predetermined portion of the encrypted information to be recorded on the recording medium, dispersion of the random-data insertion positions can make it difficult to read the random data and it is possible to effect the strong copy protect on the

information.

According to the encrypting method of the present invention, since the third encryption key is generated from the first key generated from the information inherent in the recording medium and the second key independent of the first key and the information to be recorded on the recording medium is encrypted by using the third key, it is possible to simplify the arrangement of the encrypting apparatus and it is possible to effect the strong copy protect on the information.

According to the decrypting apparatus and method of the present invention, the encryption key is generated based on the random data to be inserted into the predetermined portion of the encrypted information to be recorded on the recording medium. By using the encryption key, the first file and the second file are respectively reproduced from the first file where the encrypted information is stored and the recording medium where the second file in which there is recorded the data indicative of the predetermined portion of the random data to be inserted into the predetermined portion of the encrypted information. Based on the data stored in the reproduced second file and indicating predetermined portion of the random data, the random data is detected from the encrypted information stored in the first file. The decryption key is generated from the detected random data. The encrypted information of the reproduced first file is decrypted by using the decryption key. Therefore, it is possible to decrypt the information protected by the strong copy protect.

According to the decrypting method of the present invention, the encryption key is generated based on the wobbling frequency of the predetermined portion of the encrypted information to be recorded on the recording medium. By using the encryption key, the first file and the second file are respectively reproduced from the first file where the encrypted information is stored and the recording medium where the second file in which there is recorded the data indicative of the predetermined portion of the predetermined portion of the encrypted information to be recorded on the recording medium. Based on the data stored in the reproduced second file and indicating a predetermined portion of the encrypted information, the wobbling frequency of the predetermined portion of the encrypted information is detected. The decryption key is generated based on the detected wobbling frequency. The encrypted information of the reproduced first file is decrypted by using the decryption key. Therefore, it is possible to decrypt the information protected by the strong copy protect.

According to the decrypting method of the present invention, the encryption key is generated based on the frequency of the predetermined portion of the wobbled pregroove or the wobbled land portion to be formed on the recording medium. By using the encryption key, the first file and the second file are respectively reproduced from the first file where the encrypted information is stored and the recording medium where the second file in which there is recorded the data indicative of the predetermined portion of the wobbled pregroove

or the wobble land portion to be formed on the recording medium. Based on the data stored in the reproduced second file and indicating predetermined portion of the wobbled pregroove or the wobbled land portion, the wobbling frequency of the predetermined portion of the pregroove or the land portion formed on the recording medium is detected. The decryption key is generated based on the detected wobbling frequency. The encrypted information of the reproduced first file is decrypted by using the decryption key. Therefore, it is possible to decrypt the information protected by the strong copy protect.

According to the decrypting method of the present invention, the encryption key is generated based on the random data selected from the predetermined portions of the random file formed of the random data generated by the predetermined pseudo random data generator. The file storing the information encrypted by using the encryption key, the file storing the data indicative of the predetermined portion of the random file formed of the random data and the random file are reproduced. Based on the file storing the data indicative of the predetermined portion of the reproduced random file, the decryption key is generated from the random data at the portions of the random file. By using the decryption key, the encryption information reproduced from the recording medium is decrypted. It is possible to decrypt the information protected by the strong copy protect.

According to the decrypting method of the present invention, by using the third key generated from the first

encryption key generated from the information inherent in the recording medium and the second key independent of the first encryption key, the information is encrypted. The first decryption key is generated from the information inherent in the recording medium where the encrypted information is recorded. The third decryption key is generated based on the first decryption key and the second decryption key recorded on the predetermined key medium and corresponding to the second encryption key. By using the third decryption key, the information encrypted by using the third encryption key and reproduced from the recording medium is decrypted. It is possible to decrypt the information protected by the strong copy protect.

Having described preferred embodiments of the present invention with reference to the accompanying drawings, it is to be understood that the present invention is not limited to the above-mentioned embodiments and that various changes and modifications can be effected therein by one skilled in the art without departing from the spirit or scope of the present invention as defined in the appended claims.

What is claimed is:

1. An encrypting method of encrypting information to be recorded by using an encryption key, comprising the steps of:

generating an encryption key based on inherent information inherent in a recording medium; and

encrypting said information to be recorded on said recording medium based on said encryption key, wherein said inherent information inherent in said recording medium is a specific information on a disk.

2. An encrypting method according to claim 1, wherein said inherent information inherent in said recording medium is a frequency of a predetermined portion of a wobbled pre groove or a wobbled land portion to be formed on said recording medium.

3. An encrypting method according to claim 2, further comprising the step of :

generating a file indicative of a predetermined portion of a wobbled pre groove or a wobbled land portion to be formed on said recording medium, wherein said file is data to be recorded on said recording medium together with a file of said encrypted information.

4. An encrypting apparatus for encrypting information to be recorded by using an encryption key, comprising:

a means for generating an encryption key based on

inherent information inherent in a recording medium; and

a means for encrypting said information to be recorded on said recording medium based on said encryption key, wherein said inherent information inherent in said recording medium is a specific information on a disk.

5. An encrypting apparatus according to claim 4, wherein said inherent information inherent in said recording medium is a frequency of a predetermined portion of a wobbled pre groove or a wobbled land portion to be formed on said recording medium.

6. An encrypting apparatus according to claim 1, further comprising:

a means for generating a file indicative of a predetermined portion of a wobbled pre groove or a wobbled land portion to be formed on said recording medium, wherein said file is data to be recorded on said recording medium together with a file of said encrypted information.

7. A recording method of recording on a recording medium information obtained by encrypting information to be recorded by using an encryption key, comprising the steps of:

receiving an encrypted information based on an encryption key generated based on inherent information inherent in a recording medium; and

recording said received encrypted information on a

recording medium, wherein said inherent information inherent in said recording medium is a specific information on a disk.

8. A recording method according to claim 7, wherein said inherent information inherent in said recording medium is a frequency of a predetermined portion of a wobbled pre groove or a wobbled land portion to be formed on said recording medium

9. A recording method according to claim 8, wherein a file indicative of a predetermined portion of said wobbled pregroove or wobbled land portion to be formed on said recording medium is received and said file is recorded on said recording medium together with a file of said encrypted information.

10. An encrypting method of encrypting information to be recorded by using an encryption key, comprising the steps of:

generating an encryption key based on inherent information inherent in a recording medium; and

encrypting said information to be recorded on said recording medium based on said encryption key, wherein said inherent information inherent in said recording medium is a random data inserted into a predetermined portion of said encrypted information to be recorded on said recording medium.

11. An encrypting method according to claim 10, further comprising the step of:

generating a file indicative of a predetermined

portion of a random data inserted into a predetermined portion of said encrypted information to be recorded on said recording medium, wherein said file is data to be recorded on said recording medium together with a file of said encrypted information.

12. An encrypting method according to claim 10, wherein said random data is data to be recorded on said recording medium as a normal file according to ISO9660 standard.

13. An encrypting method according to claim 10, wherein said random data is data to be recorded on said recording medium as an interleaved file.

14. An encrypting method according to claim 10, wherein said random data is data to be recorded on said recording medium as a multi extent file.

15. An encrypting method according to claim 10, wherein said random data is data to be recorded on a pre gap area of a file according to ISO9660 standard.

16. An encrypting method according to claim 10, wherein said random data is data to be recorded on a system area of a file according to ISO9660 standard.

17. An encrypting method according to claim 10,

wherein said random data is data to be recorded on an application area of a primary volume descriptor of a file according to ISO9660 standard.

18. An encrypting method according to claim 10, wherein said random data is data to be recorded on a surface of said recording medium.

19. An encrypting method according to claim 10, wherein said random data is random data selected from a predetermined portion of a random file generated by a predetermined pseudo random generator.

20. An encrypting method according to claim 19, wherein a file indicative of said predetermined portion of said random file formed of said random data and said random file are recorded on said recording medium together with a file of said encrypted information.

21. An encrypting apparatus for encrypting information to be recorded by using an encryption key, comprising:

a means for generating an encryption key based on inherent information inherent in a recording medium; and

a means for encrypting said information to be recorded on said recording medium based on said encryption key, wherein said inherent information inherent in said recording

medium is a random data inserted into a predetermined portion of said encrypted information to be recorded on said recording medium.

22. An encrypting apparatus according to claim 21, further comprising:

a means for generating a file indicative of a predetermined portion of a random data inserted into a predetermined portion of said encrypted information to be recorded on said recording medium, wherein said file is data to be recorded on said recording medium together with a file of said encrypted information.

23. An encrypting method according to claim 21, wherein said random data is data to be recorded on said recording medium as a normal file according to ISO9660 standard.

24. A recording method of recording on a recording medium information obtained by encrypting information to be recorded by using an encryption key, comprising the steps of:

receiving an encrypted information based on an encryption key generated based on inherent information inherent in a recording medium; and

recording said received encrypted information on said recording medium, wherein said inherent information inherent in said recording medium is a random data inserted into a predetermined portion of said encrypted information to be

recorded on said recording medium.

25. A recording method according to claim 24, wherein a file of said encrypted information and a file indicative of a predetermined portion of said random data inserted into a predetermined portion of said encrypted information to be recorded on said recording medium are recorded on said recording medium.

26. A recording method according to claim 24, wherein said random data is random data selected from a predetermined portion of a random file generated by a predetermined pseudo random generator.

27. A recording method according to claim 26, wherein a file indicative of said predetermined portion of said random file formed of said random data and said random file are recorded on said recording medium together with a file of said encrypted information.

28. A recording method according to claim 24, wherein said random data is data to be recorded on said recording medium as a file according to ISO9660 standard.

29. A recording method of recording on a recording medium information obtained by encrypting information to be recorded by using an encryption key, comprising the steps of:

receiving an encrypted information based on an encryption key generated based on inherent information inherent in a recording medium; and

recording said received encrypted information on said recording medium, wherein said inherent information inherent in said recording medium is recorded on a surface of said recording medium.

30. An encrypting method of encrypting information to be recorded by using an encryption key, comprising the steps of:

generating a third encryption key from a first encryption key generated from information inherent in a recording medium and a second encryption key independent of said first encryption key; and

encrypting information to be recorded on said recording medium by using said third encryption key.

31. An encrypting method according to claim 30, wherein said inherent information inherent in said recording medium is a frequency of a predetermined portion of a wobbled pregroove or a wobbled land portion to be formed on said recording medium.

32. An encrypting method according to claim 30, wherein said inherent information inherent in said recording medium is random data inserted in to a predetermined portion of said encrypted information to be recorded on said recording

medium.

33. An encrypting apparatus for encrypting information to be recorded by using an encryption key, comprising:

a means for generating a third encryption key from a first encryption key generated from information inherent in a recording medium and a second encryption key independent of said first encryption key; and

a means for encrypting information to be recorded on said recording medium by using said third encryption key.

34. An encrypting apparatus according to claim 33, wherein said inherent information inherent in said recording medium is a frequency of a predetermined portion of a wobbled pregroove or a wobbled land portion to be formed on said recording medium.

35. An encrypting apparatus according to claim 33, wherein said inherent information inherent in said recording medium is random data inserted in to a predetermined portion of said encrypted information to be recorded on said recording medium.

36. A recording method of recording on a recording medium information obtained by encrypting information to be recorded by using an encryption key, comprising the steps of:

receiving an encrypted information based on an encryption key generated based on a third encryption key generated from a first encryption key generated from information inherent in a recording medium and a second encryption key independent of said first encryption key; and

recording said received encrypted information on a recording medium.

37. A decrypting method of decrypting an encrypted information recorded on a recording medium, comprising the steps of:

reproducing a first file storing information encrypted by using an encryption key generated based on a random data to be inserted into a predetermined portion of said encrypted information to be recorded on a recording medium and a second file storing data indicative of a predetermined portion of said random data to be inserted into a predetermined portion of said encrypted information, from said recording medium;

detecting said random data from said encrypted information stored in said reproduced first file based on said data stored in said reproduced second file and indicating said predetermined portion of said random data;

generating a decryption key from said detected random data; and

decrypting said encrypted information of said reproduced first file by using said decryption key.

38. A decrypting method of decrypting an encrypted information recorded on a recording medium, comprising the steps of:

reproducing from a recording medium a first file storing information encrypted by using an encryption key generated based on a wobbling frequency of a predetermined portion of said information to be recorded on a recording medium and a second file storing data indicative of a predetermined portion of said encrypted information to be recorded on said recording medium;

detecting said wobbling frequency of a predetermined portion of said information stored in said reproduced first file based on said data stored in said reproduced second file and indicating said predetermined portion of said encrypted information;

generating a decryption key from said detected wobbling frequency; and

decrypting said encrypted information of said reproduced first file by using said decryption key.

39. A decrypting method of decrypting an encrypted information recorded on a recording medium, comprising the steps of:

reproducing from a recording medium a first file storing information encrypted by using an encryption key generated based on a frequency of a predetermined portion of a wobbled pregroove or a wobbled land portion to be formed on a

recording medium and a second file storing data indicative of a predetermined portion of said wobbled pregroove or wobbled land portion to be formed on said recording medium;

detecting said wobbling frequency of a predetermined portion of said pregroove or land portion formed on sid recording medium based on said data stored in said reproduced second file and indicating said predetermined portion of said wobbled pregroove or said wobbled land portion;

generating a decryption key from said detected wobbling frequency; and

decrypting said encrypted information stored in said reproduced first file by using said decryption key.

40. A decrypting method of decrypting an encrypted information recorded on a recording medium, comprising the steps of:

reproducing a file storing information encrypted by using an encryption key generated based on a random data selected from a predetermined portion of a random file formed of said random data generated by a predetermined pseudo random data generator, a file storing data indicative of a predetermined portion of said random file formed of said random data, and said random file;

generating a decryption key from said random data of said predetermined portion obtained from said random file based on said file storing data indicative of a predetermined portion of said reproduced random file; and

decrypting said reproduced encrypted information by using said decryption key.

41. A decrypting method of decrypting an encrypted information recorded on a recording medium, comprising the steps of:

generating a first decryption key from inherent information inherent in a recording medium where there is recorded information encrypted by a third encryption key generated based on a first encryption key generated from said inherent information inherent in said recording medium and a second encryption key independent of said first encryption key;

generating a third decryption key based on a second decryption key recorded on a predetermined key medium and corresponding to said second encryption key and said first decryption key; and

decrypting said information encrypted by using said third encryption key and reproduced from said recording medium, by using said third decryption key.

42. A decrypting method according to claim 41, wherein said key medium is a card where said second decryption key is recorded magnetically or optically.

43. A decrypting method according to claim 41, wherein said key medium comprises a memory storing said second decryption key.

44. A decrypting apparatus for decrypting an encrypted information recorded on a recording medium, comprising:

a means for reproducing from said recording medium a first file storing information encrypted by using an encryption key generated based on a random data to be inserted into a predetermined portion of said encrypted information to be recorded on a recording medium and a second file storing data indicative of a predetermined portion of said random data to be inserted into a predetermined portion of said encrypted information;

a means for detecting said random data from said encrypted information stored in said reproduced first file based on said data stored in said reproduced second file and indicating said predetermined portion of said random data;

a means for generating a decryption key from said detected random data; and

a means for decrypting said encrypted information of said reproduced first file by using said decryption key.

45. A decrypting apparatus for decrypting an encrypted information recorded on a recording medium, comprising:

a means for reproducing from a recording medium a first file storing information encrypted by using an encryption key generated based on a wobbling frequency of a predetermined

portion of said information to be recorded on a recording medium and a second file storing data indicative of a predetermined portion of said encrypted information to be recorded on said recording medium;

a means for detecting said wobbling frequency of a predetermined portion of said information stored in said reproduced first file based on said data stored in said reproduced second file and indicating said predetermined portion of said encrypted information;

a means for generating a decryption key from said detected wobbling frequency; and

a means for decrypting said encrypted information of said reproduced first file by using said decryption key.

46. A decrypting apparatus for decrypting an encrypted information recorded on a recording medium, comprising:

a means for reproducing from a recording medium a first file storing information encrypted by using an encryption key generated based on a frequency of a predetermined portion of a wobbled pregroove or a wobbled land portion to be formed on a recording medium and a second file storing data indicative of a predetermined portion of said wobbled pregroove or wobbled land portion to be formed on said recording medium;

a means for detecting a wobbling frequency of a predetermined portion of said pregroove or land portion formed on said recording medium based on said data stored in said

reproduced second file and indicating said predetermined portion of said wobbled pregroove or said wobbled land portion;

a means for generating a decryption key from said detected wobbling frequency; and

a means for decrypting said encrypted information stored in said reproduced first file by using said decryption key.

47. A decrypting apparatus for decrypting an encrypted information recorded on a recording medium, comprising:

a means for reproducing a file storing information encrypted by using an encryption key generated based on a random data selected from a predetermined portion of a random file formed of said random data generated by a predetermined pseudo random data generator and recorded on a predetermined recording medium, a file storing data indicative of a predetermined portion of said random file formed of said random data, and said random file;

a means for generating a decryption key from said random data of said predetermined portion obtained from said random file based on said file storing data indicative of a predetermined portion of said reproduced random file; and

a means for decrypting said reproduced encrypted information by using said decryption key.

48. A decrypting apparatus for decrypting an

encrypted information recorded on a recording medium, comprising:

a means for generating a first decryption key from inherent information inherent in a recording medium where there is recorded information encrypted by a third encryption key generated based on a first encryption key generated from said inherent information inherent in said recording medium and a second encryption key independent of said first encryption key;

a means for generating a third decryption key based on a second decryption key recorded on a predetermined key medium and corresponding to said second encryption key and said first decryption key; and

a means for decrypting said information encrypted by using said third encryption key and reproduced from said recording medium, by using said third decryption key.

49. A decrypting apparatus according to claim 48, wherein said key medium is a card where said second decryption key is recorded magnetically or optically.

50. A decrypting apparatus according to claim 48, wherein said key medium comprises a memory storing said second decryption key.

51. A recording medium capable of being used in decryption by a decrypting apparatus, comprising:

a recorded signal capable of being decrypted by a

decrypting apparatus, wherein said recorded signal comprises a first file storing information encrypted by using an encryption key generated based on random data to be inserted into a predetermined portion of an encrypted information.

52. A recording medium according to claim 51, wherein said recorded signal further comprises a second file storing data indicative of a predetermined portion of said random data to be inserted into a predetermined portion of said encrypted information.

53. A recording medium capable of being used in decryption by a decrypting apparatus, comprising:

a recorded signal capable of being decrypted by a decrypting apparatus, wherein said recorded signal comprises a first file storing information encrypted by using an encryption key generated based on a wobbling frequency of a predetermined portion of a recording medium.

54. A recording medium according to claim 53, wherein said recorded signal further comprises a second file storing data indicative of a predetermined portion of said encrypted information to be recorded on said recording medium.

55. A recording medium capable of being used in decryption by a decrypting apparatus, comprising:

a recorded signal capable of being decrypted by a

decrypting apparatus, wherein said recorded signal comprises a first file storing information encrypted by using an encryption key generated based on a frequency of a predetermined portion of a wobbled pregroove or a wobbled land portion to be formed on a recording medium.

56. A recording medium according to claim 55, wherein said recorded signal further comprises a second file storing data indicative of a predetermined portion of a wobbled pregroove or a wobbled land portion to be formed on a recording medium.

57. A recording medium capable of being used in decryption by a decrypting apparatus, comprising:

a recorded signal capable of being decrypted by a decrypting apparatus, wherein said recorded signal comprises a file storing information encrypted by using an encryption key generated based on a random data selected from a predetermined portion of a random file formed of said random data generated by a predetermined pseudo random generator.

58. A recording medium according to claim 57, wherein said recorded signal further comprises a second file storing data indicative of a predetermined portion of a random file formed of said random data.

59. A recording medium capable of being used in

decryption by a decrypting apparatus, comprising:

a recorded signal capable of being decrypted by a decrypting apparatus, wherein said recorded signal comprises information encrypted by using a third encryption key generated based on a first encryption key generated from inherent information inherent in a recording medium and a second encryption key independent of said first encryption key.

ABSTRACT OF THE DISCLOSURE

When information to be recorded is encrypted by using an encryption key, an encryption key based on inherent information inherent in a recording medium is generated. The information to be recorded on the recording medium is encrypted based on the encryption key. The inherent information inherent in the recording medium is a specific information on a disk. When an encrypted information recorded on a recording medium is decrypted, there are reproduced from a recording medium a first file storing information encrypted by using an encryption key generated based on a random data to be inserted into a predetermined portion of the encrypted information to be recorded on a recording medium and a second file storing data indicative of a predetermined portion of the random data to be inserted into a predetermined portion of the encrypted information. The random data is detected from the encrypted information stored the reproduced first file based on the data stored in the reproduced second file and indicating the predetermined portion of the random data. A decryption key is generated from the detected random data. The encrypted information of the reproduced first file is decrypted by using the decryption key.

FIG. 1

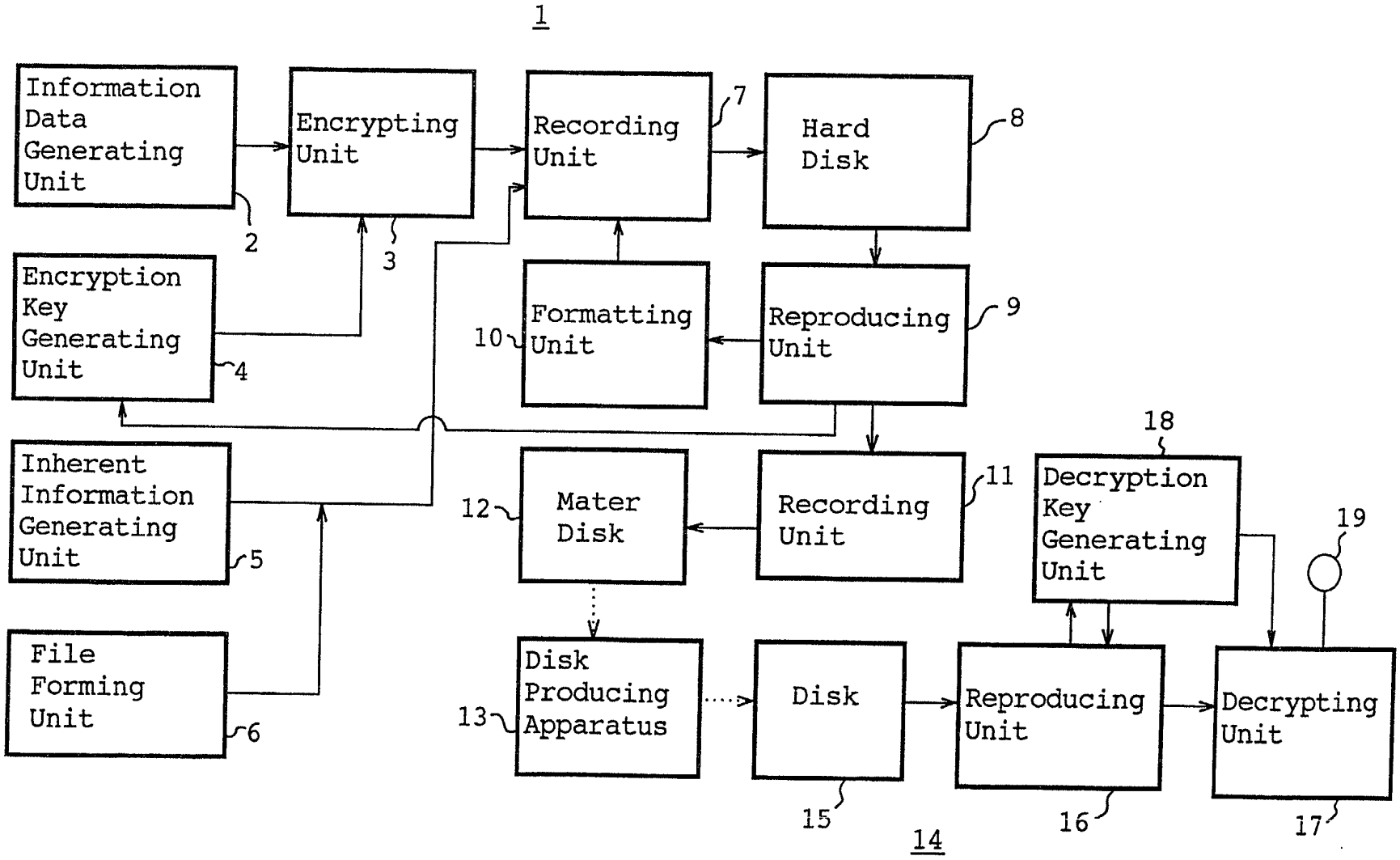

1
Information Data Generating Unit
2
Encrypting Unit
3
Recording Unit
7
Hard Disk
8
Encryption Key Generating Unit
4
Formatting Unit
10
Reproducing Unit
9
Inherent Information Generating Unit
5
Mater Disk
12
Recording Unit
11
18
Decryption Key Generating Unit
19
File Forming Unit
6
Disk Producing Apparatus
13
Disk
15
Reproducing Unit
16
Decrypting Unit
17
14

FIG. 2

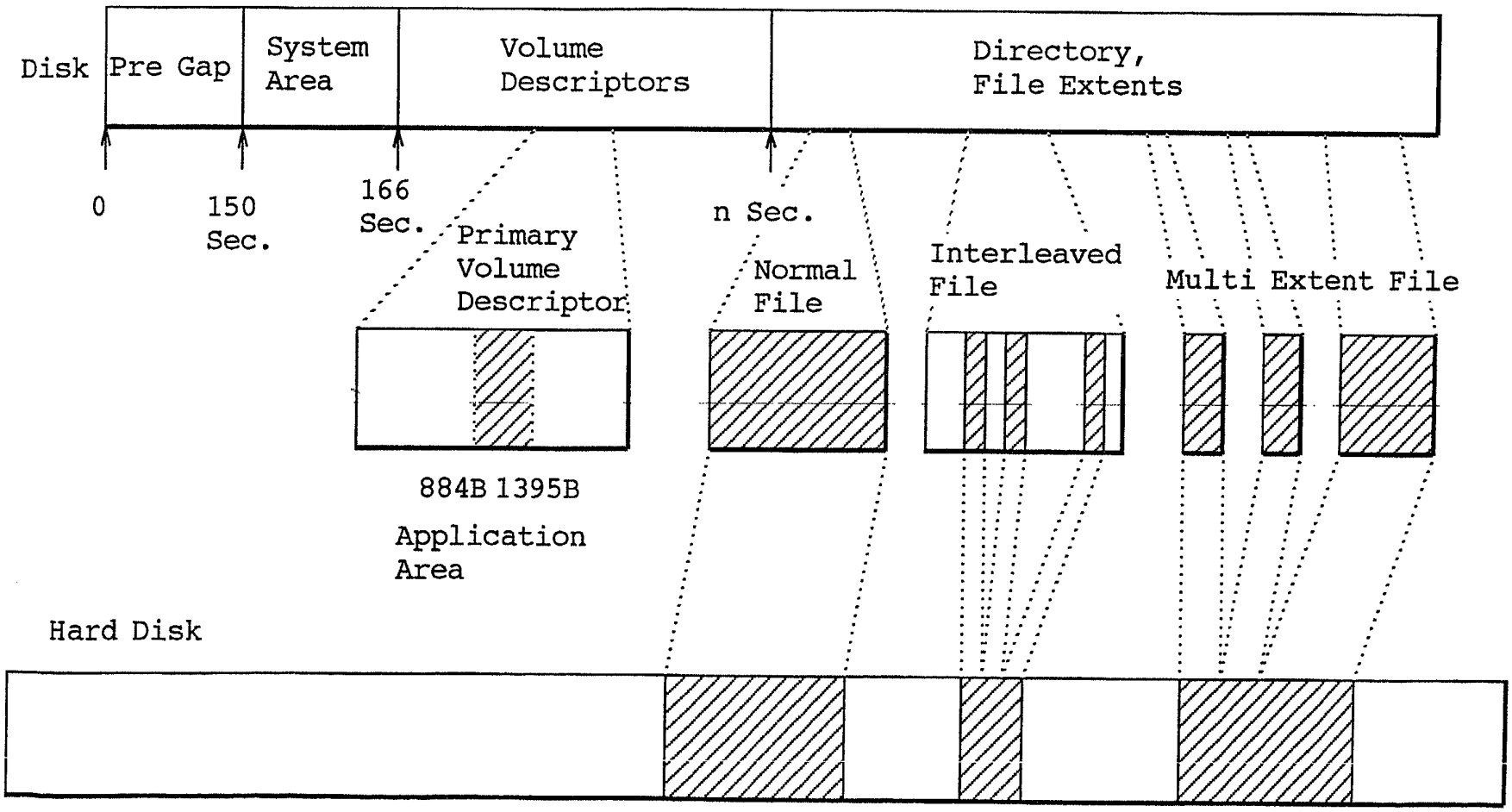

Disk
Pre Gap
System Area
Volume Descriptors
Directory, File Extents
0
150 Sec.
166 Sec.
n Sec.
Primary Volume Descriptor
Normal File
Interleaved File
Multi Extent File
884B 1395B
Application Area
Hard Disk

FIG. 3

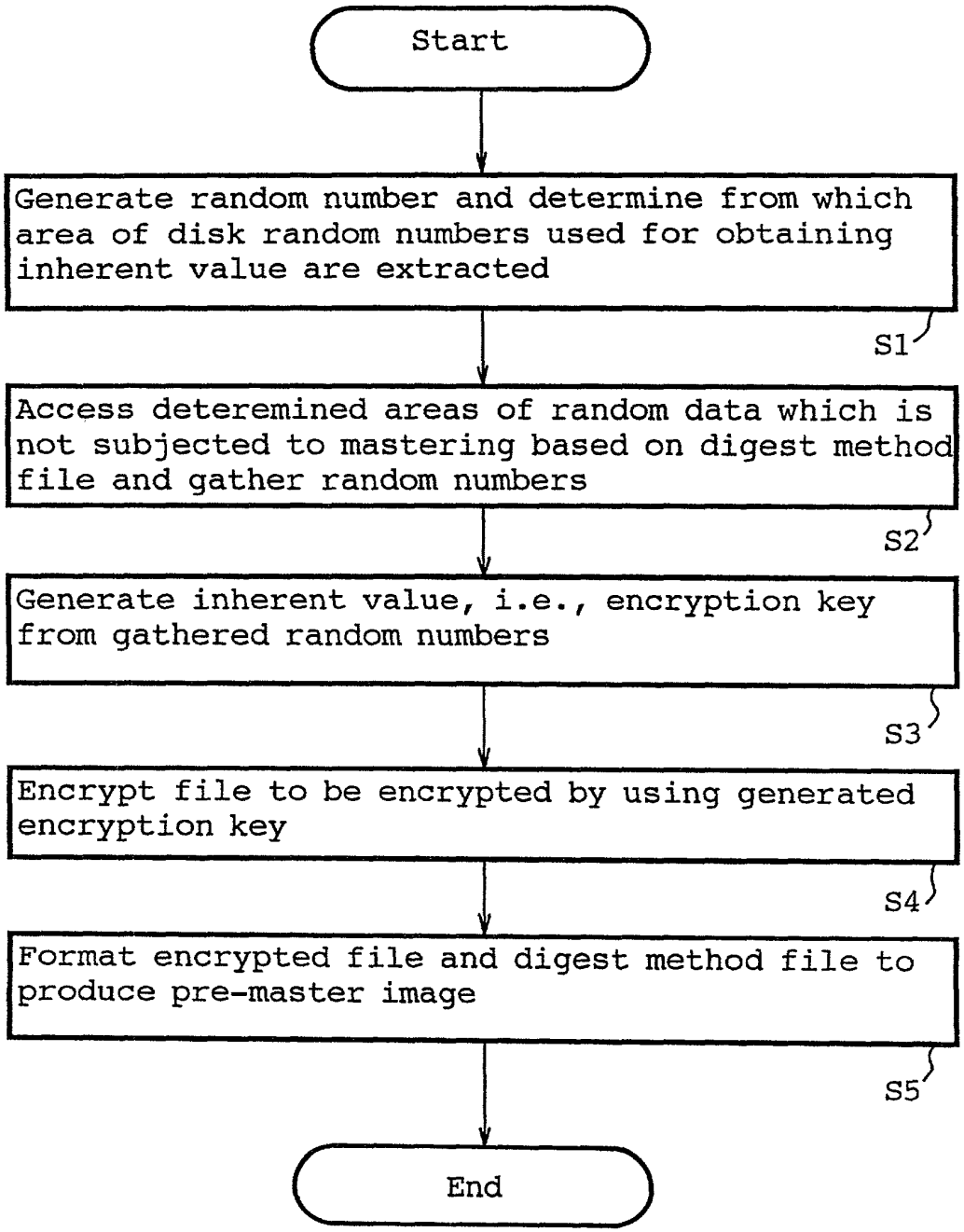


FIG. 4

Sector number 1 / Offset
Sector number 2 / Offset
Sector number 3 / Offset
. . . .
Sector number (n-1) / Offset
Sector number n / Offset

FIG. 5

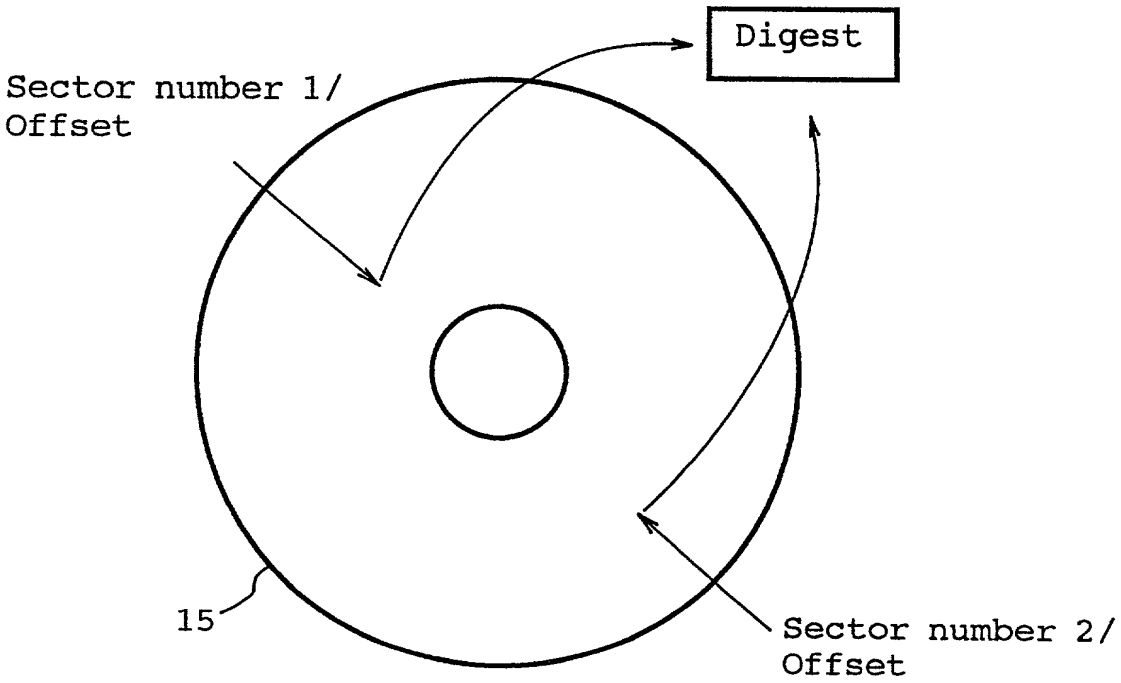


FIG. 6

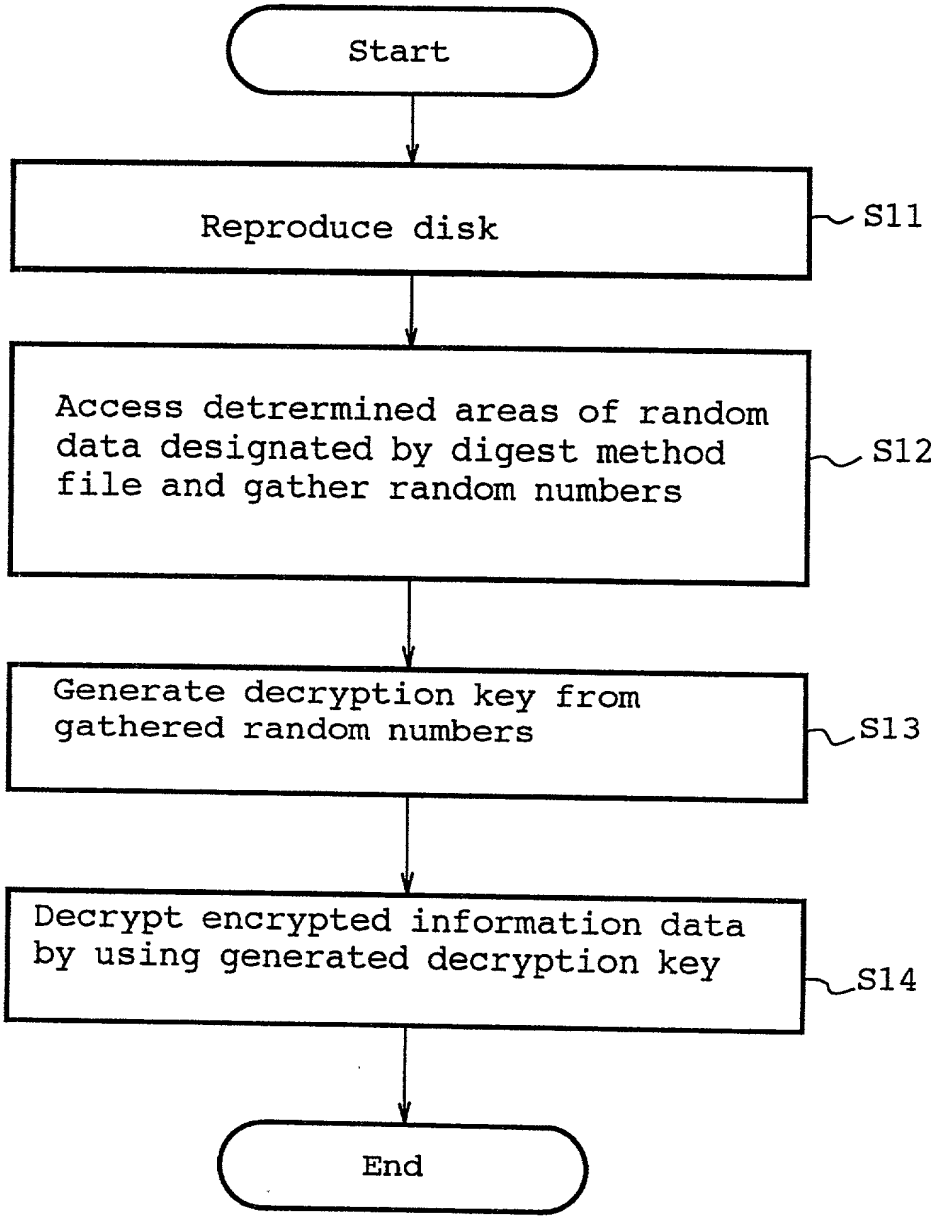

Start
Reproduce disk
S11
Access detrermined areas of random data designated by digest method file and gather random numbers
S12
Generate decryption key from gathered random numbers
S13
Decrypt encrypted information data by using generated decryption key
S14
End

FIG. 7

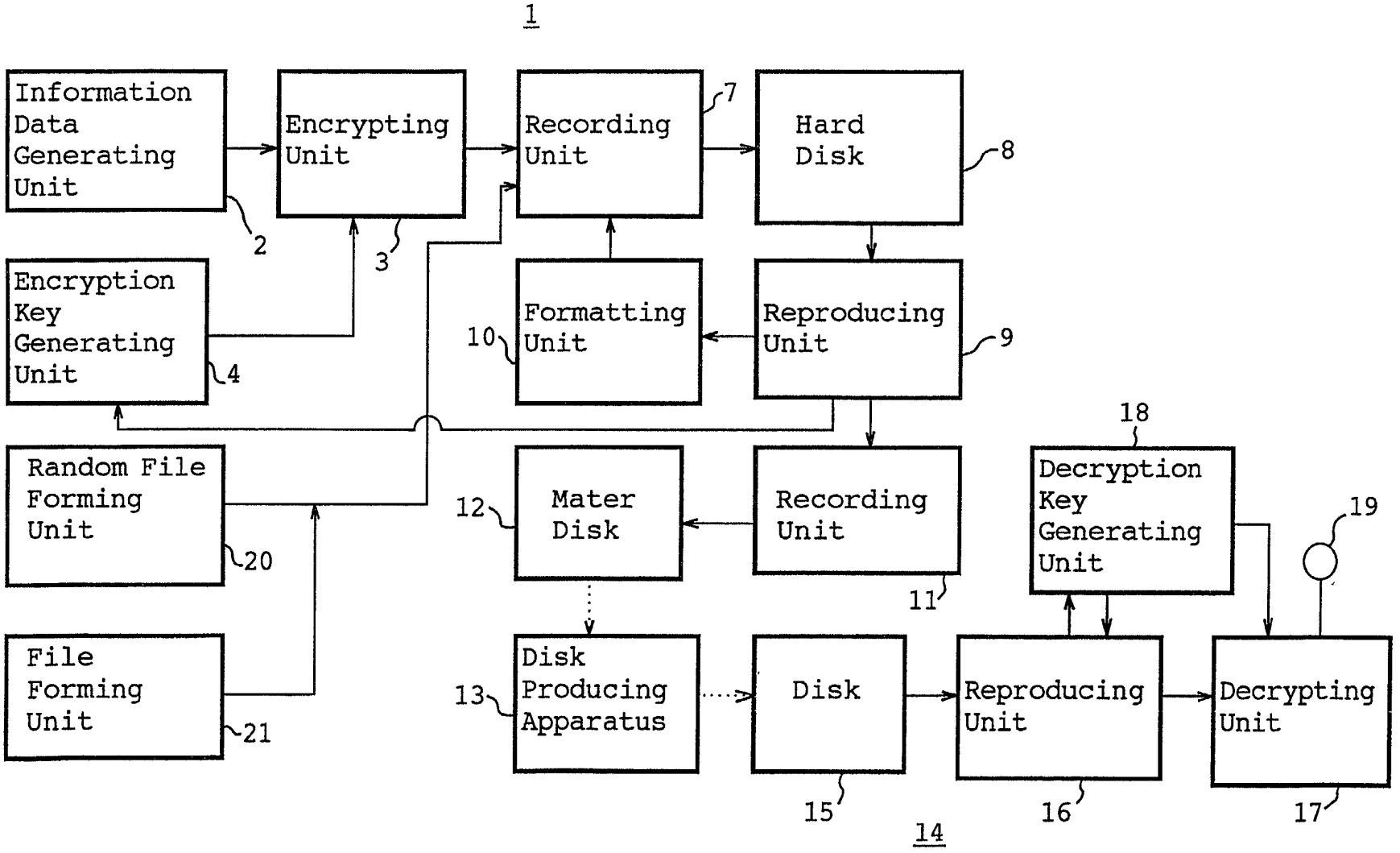

1
Information Data Generating Unit
2
Encrypting Unit
3
Recording Unit
7
Hard Disk
8
Encryption Key Generating Unit
4
Formatting Unit
10
Reproducing Unit
9
Random File Forming Unit
20
Mater Disk
12
Recording Unit
11
18
Decryption Key Generating Unit
19
File Forming Unit
21
Disk Producing Apparatus
13
Disk
15
Reproducing Unit
16
Decrypting Unit
17
14

FIG. 8

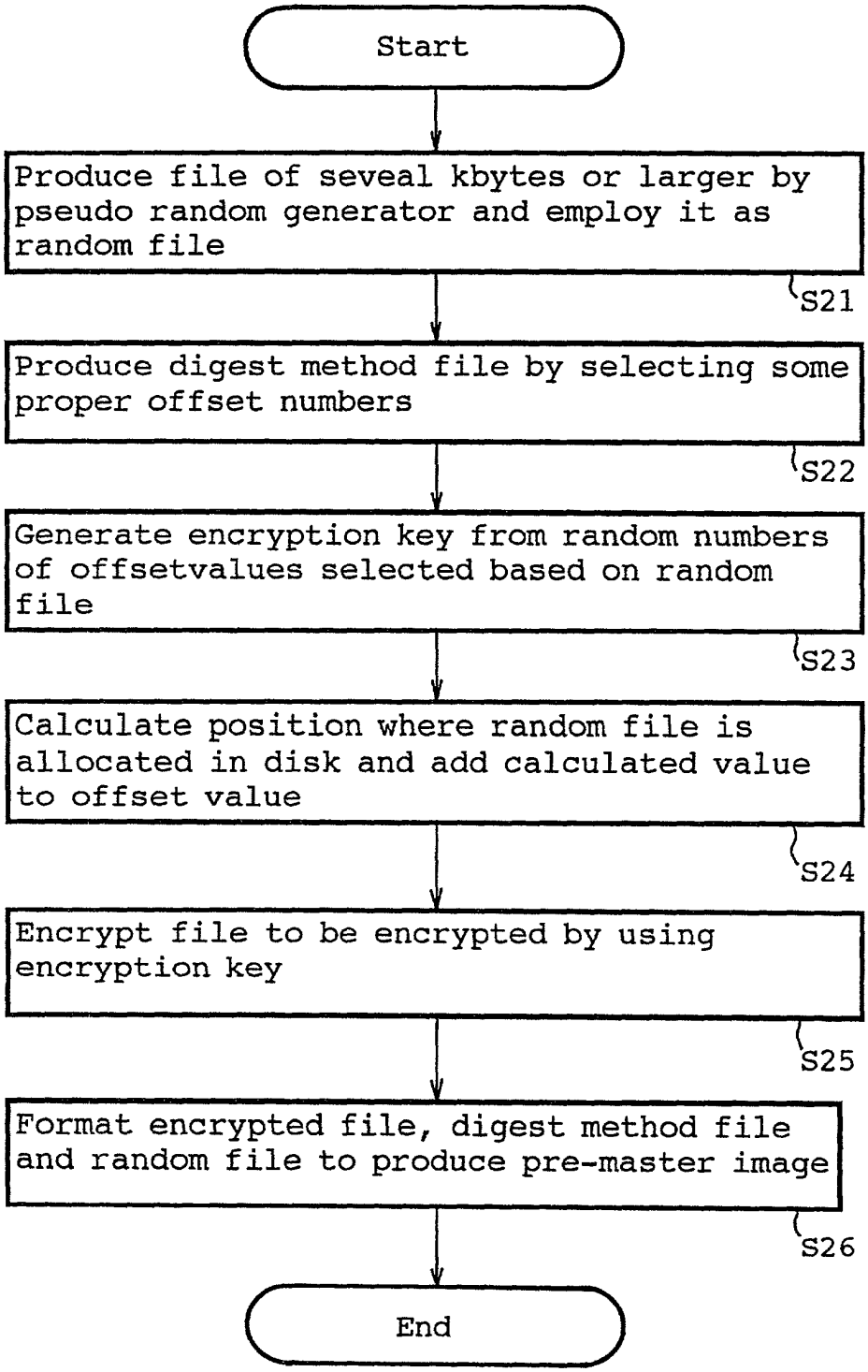

Start
Produce file of seveal kbytes or larger by pseudo random generator and employ it as random file
S21
Produce digest method file by selecting some proper offset numbers
S22
Generate encryption key from random numbers of offsetvalues selected based on random file
S23
Calculate position where random file is allocated in disk and add calculated value to offset value
S24
Encrypt file to be encrypted by using encryption key
S25
Format encrypted file, digest method file and random file to produce pre-master image
S26
End

FIG. 9

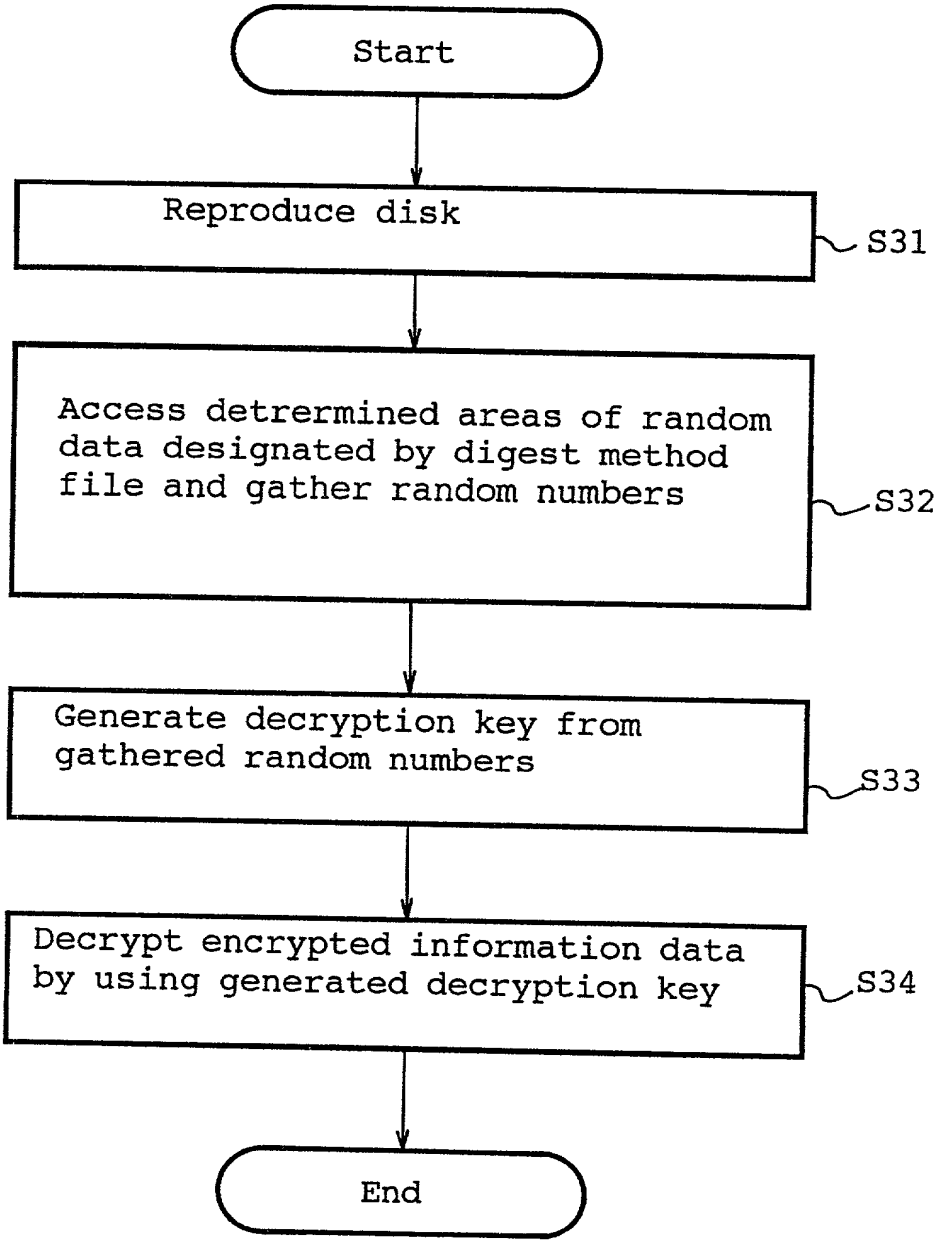

Start
Reproduce disk
S31
Access detrermined areas of random data designated by digest method file and gather random numbers
S32
Generate decryption key from gathered random numbers
S33
Decrypt encrypted information data by using generated decryption key
S34
End

FIG. 10

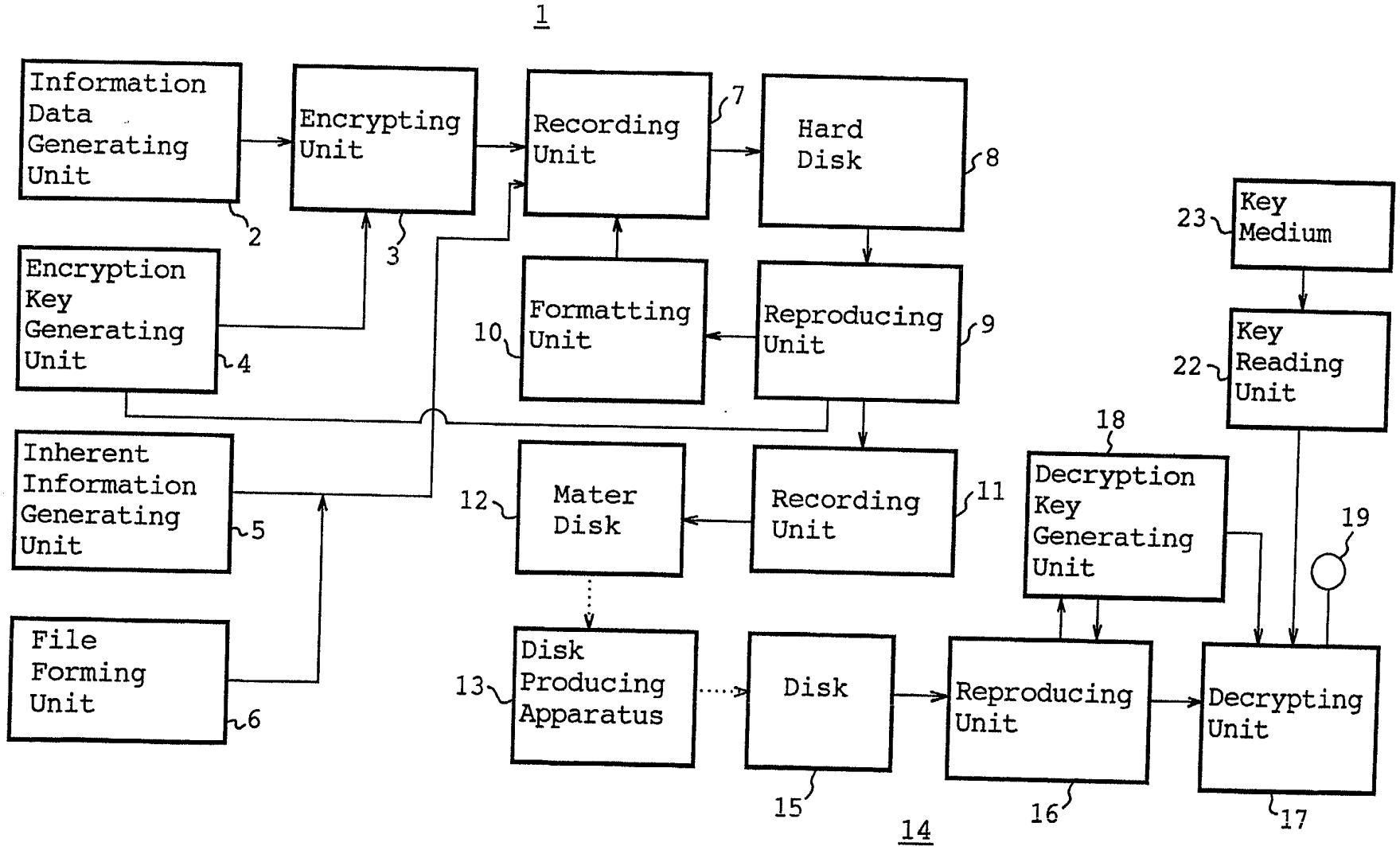

1
Information Data Generating Unit
2
Encrypting Unit
3
Recording Unit
7
Hard Disk
8
Encryption Key Generating Unit
4
Formatting Unit
10
Reproducing Unit
9
Inherent Information Generating Unit
5
Mater Disk
12
Recording Unit
11
File Forming Unit
6
Disk Producing Apparatus
13
Disk
15
Reproducing Unit
16
Decrypting Unit
17
14
Key Medium
23
Key Reading Unit
22
18
Decryption Key Generating Unit
19

FIG. 11

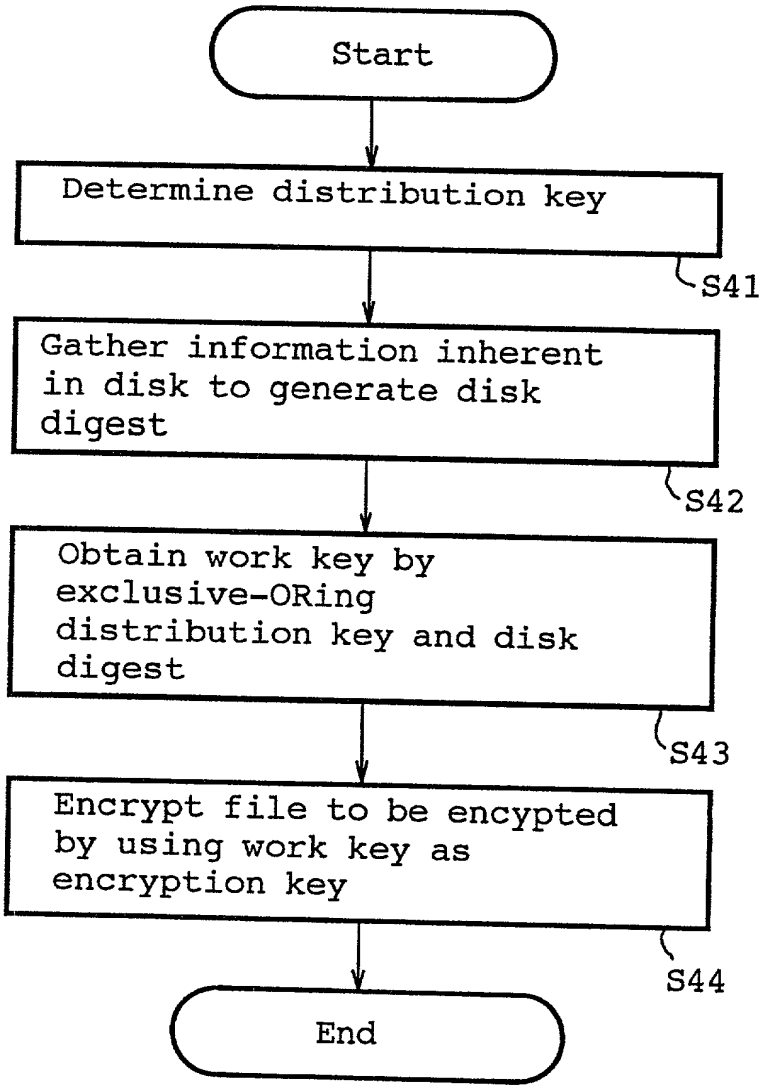

Start
Determine distribution key
S41
Gather information inherent in disk to generate disk digest
S42
Obtain work key by exclusive-ORing distribution key and disk digest
S43
Encrypt file to be encypted by using work key as encryption key
S44
End

FIG. 12

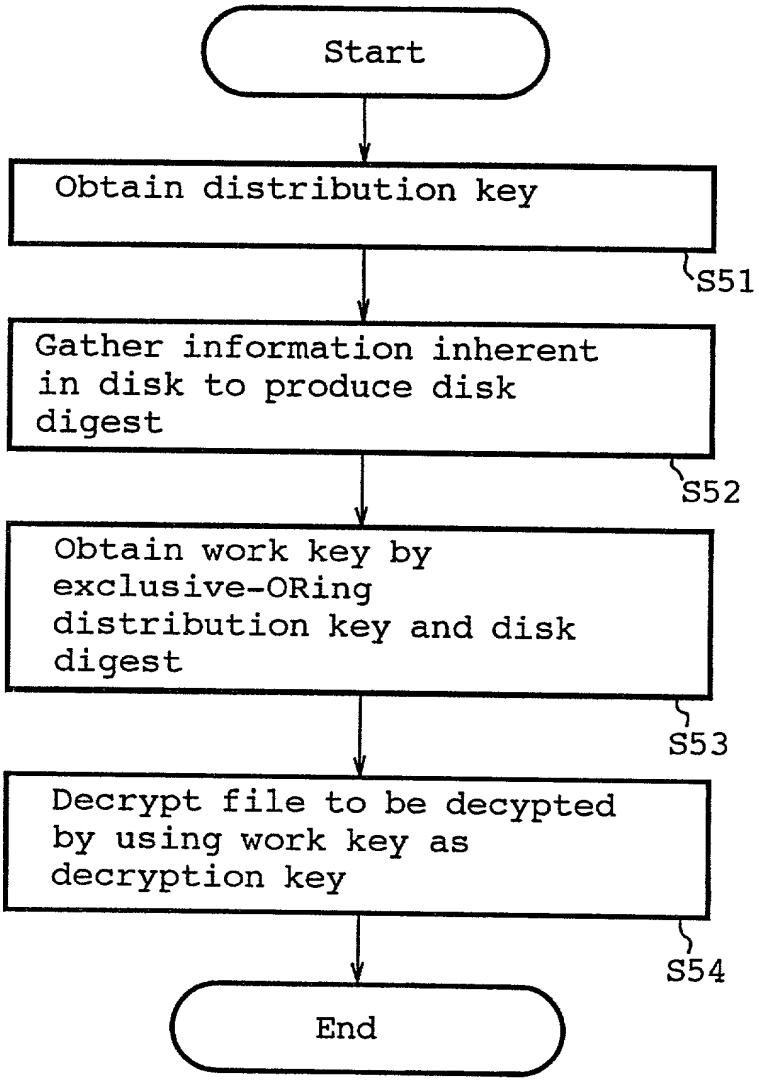

Start
Obtain distribution key
S51
Gather information inherent in disk to produce disk digest
S52
Obtain work key by exclusive-ORing distribution key and disk digest
S53
Decrypt file to be decypted by using work key as decryption key
S54
End

FIG. 13

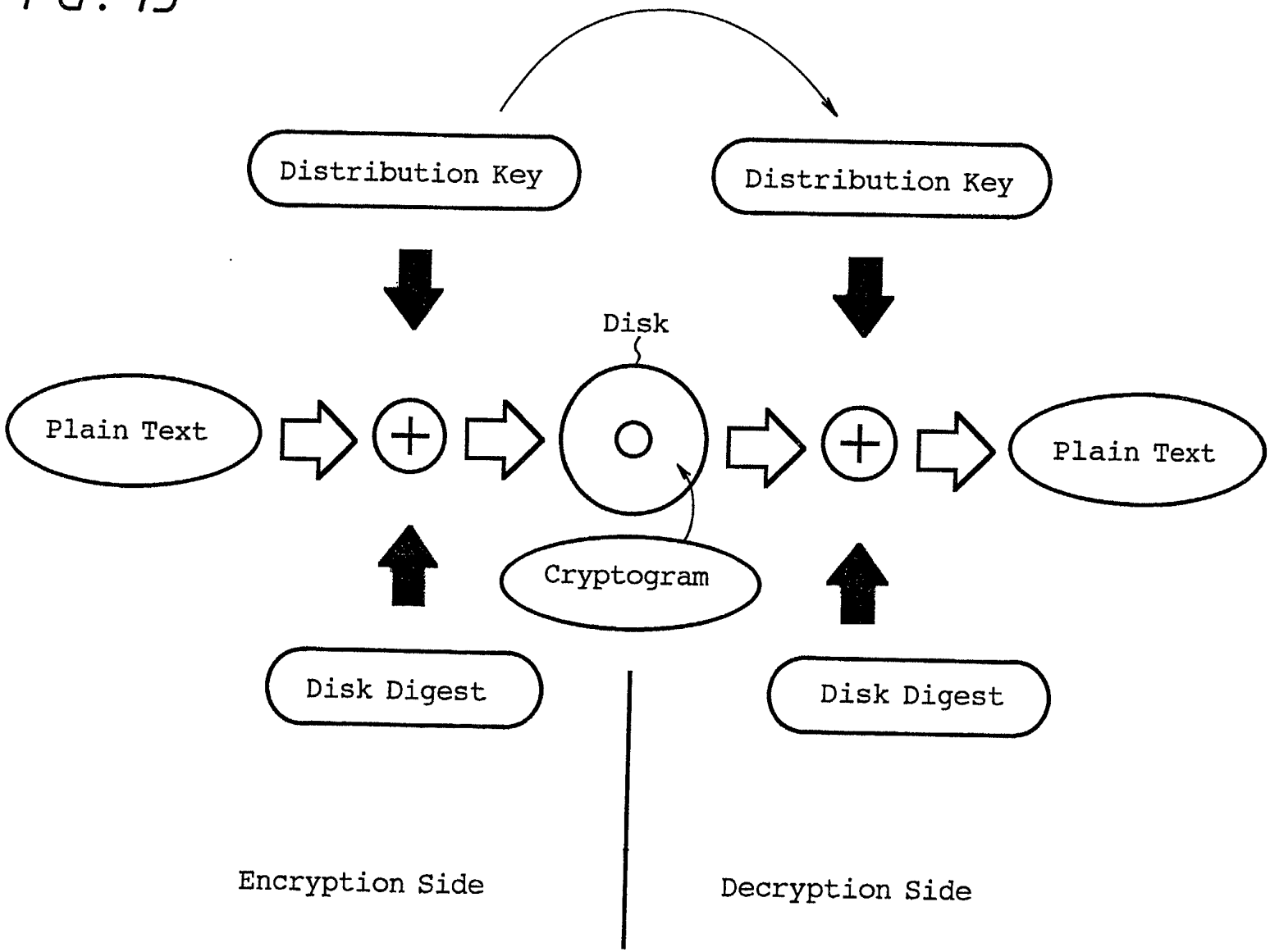

Distribution Key
Distribution Key
Disk
Plain Text
Plain Text
Cryptogram
Disk Digest
Disk Digest
Encryption Side
Decryption Side

FIG. 14

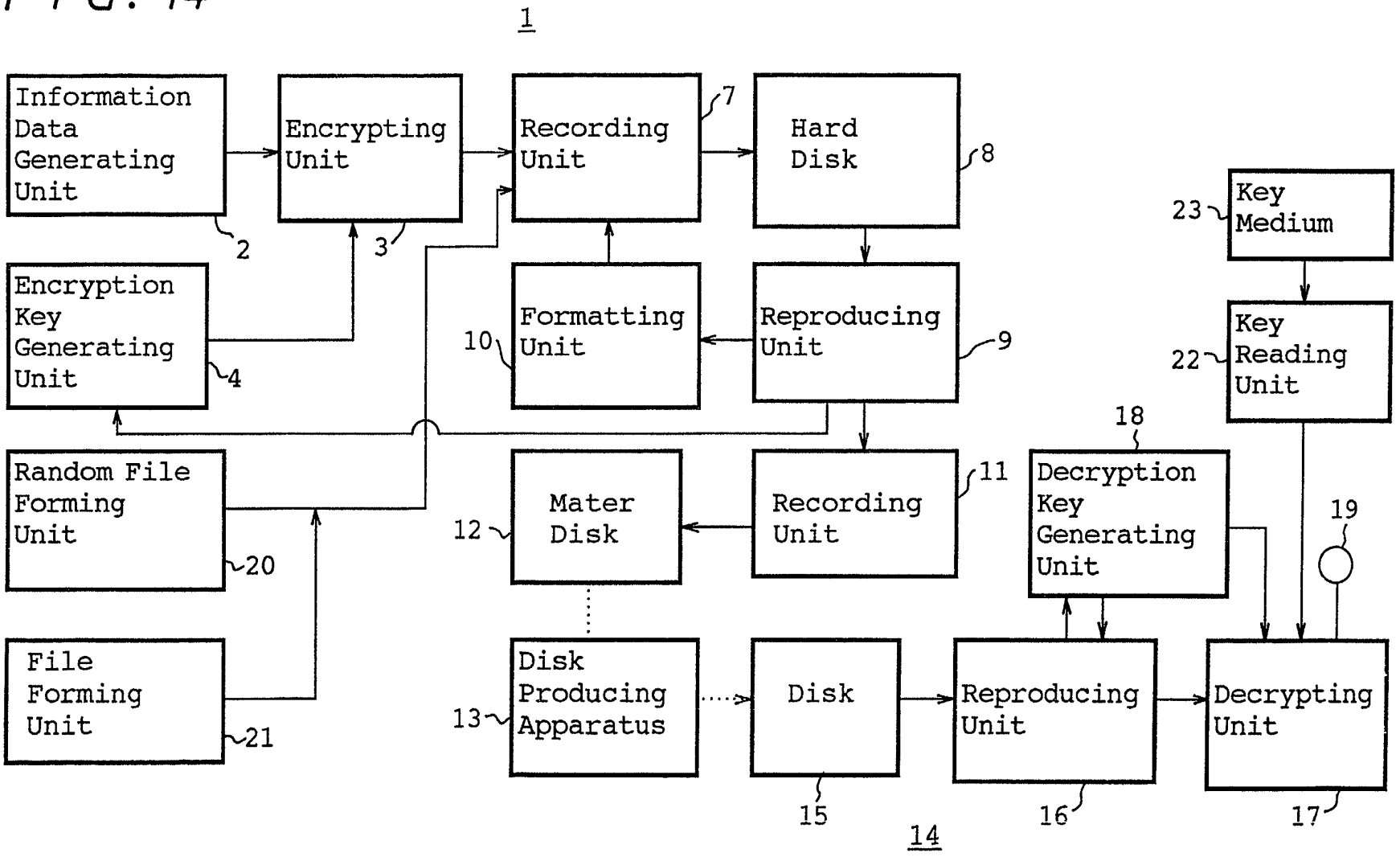
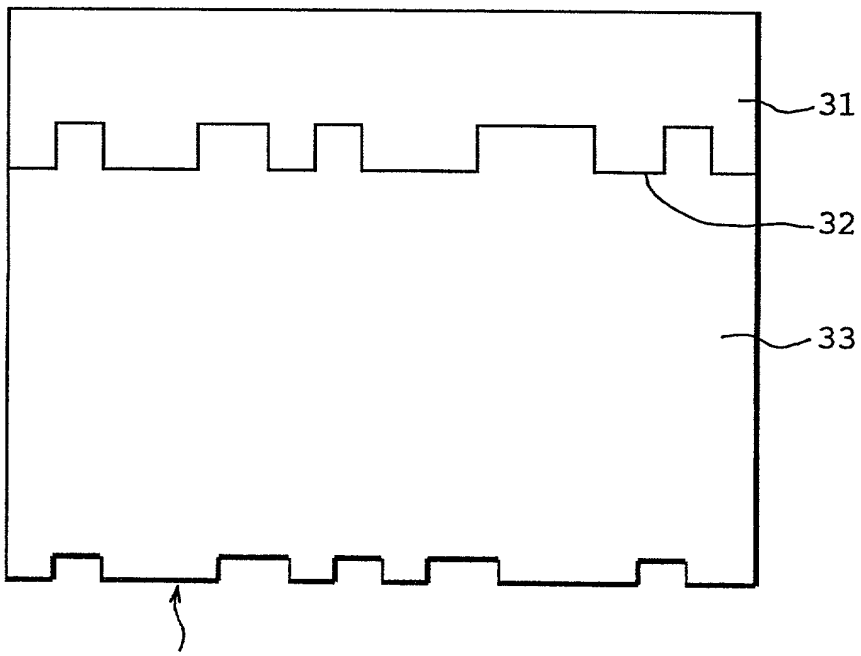

1
Information Data Generating Unit
2
Encrypting Unit
3
Recording Unit
7
Hard Disk
8
Key Medium
23
Key Reading Unit
22
Encryption Key Generating Unit
4
Formatting Unit
10
Reproducing Unit
9
18
Decryption Key Generating Unit
19
Random File Forming Unit
20
Mater Disk
12
Recording Unit
11
File Forming Unit
21
Disk Producing Apparatus
13
Disk
15
Reproducing Unit
16
Decrypting Unit
17
14

FIG. 15


31
32
33
Information inherent in disk which is recorded on surface of substrate

PATENT
450100-3689.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s)	:	Ryuji Ishiguro et al.
Serial No.	:	Continuation of Serial No. 08/721,310
For	:	ENCRYPTING METHOD AND APPARATUS, RECORDING METHOD, DECRYPTING METHOD AND APPARATUS, AND RECORDING MEDIUM
Filed	:	Herewith
Examiner	:	P. M. Laufer
Art Unit	:	2766

745 Fifth Avenue
New York, NY 10151

EXPRESS MAIL

Mailing Label Number: EM009638395US

Date of Deposit: April 7, 1999

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to: Assistant Commissioner for Patents, Washington, DC 20231.

Charles Jackson
(Typed or printed name of person mailing paper or fee)

Charles Jackson
(Signature of person mailing paper or fee)

REQUEST FOR APPROVAL OF DRAWING CHANGE

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The approval of the Examiner for the following corrections, indicated in red ink on the attached copies of Figs. 1, 3, 6, 7, 9-12 and 14 is requested:

In Fig. 1, element 2, please delete "Information".

In Fig. 1, element 12, please change "Mater" to --Master--.

In Fig. 3, step S2, please change "deteremined" to --determined--.

In Fig. 6, step S12, please change "detrermined" to --determined--.

In Fig. 7, element 2, please delete "Information".

In Fig. 7, element 12, please change "Mater" to --Master--.

In Fig. 9, step S32, please change "detrermined" to --determined--.

In Fig. 10, element 2, please delete "Information".

In Fig. 10, element 12, please change "Mater" to --Master--.

In Fig. 11, step S44, please change "encypted" to --encrypted--.

In Fig. 12, step S12, please change "decypted" to --decrypted--.

In Fig. 14, element 2, please delete "Information".

In Fig. 14, element 12, please change "Mater" to --Master--.

Upon allowance of the application, the above-noted drawing changes will be incorporated in new formal drawings of Figs. 1, 3, 6, 7, 9-12 and 14.

Kindly charge any costs related to this drawing change to Deposit Account No. 50-0320.

Respectfully submitted,
FROMMER LAWRENCE & HAUG LLP

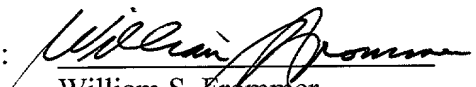
By: 
William S. Frommer
Reg. No. 25,506
(212) 588-0800

FIG. 1

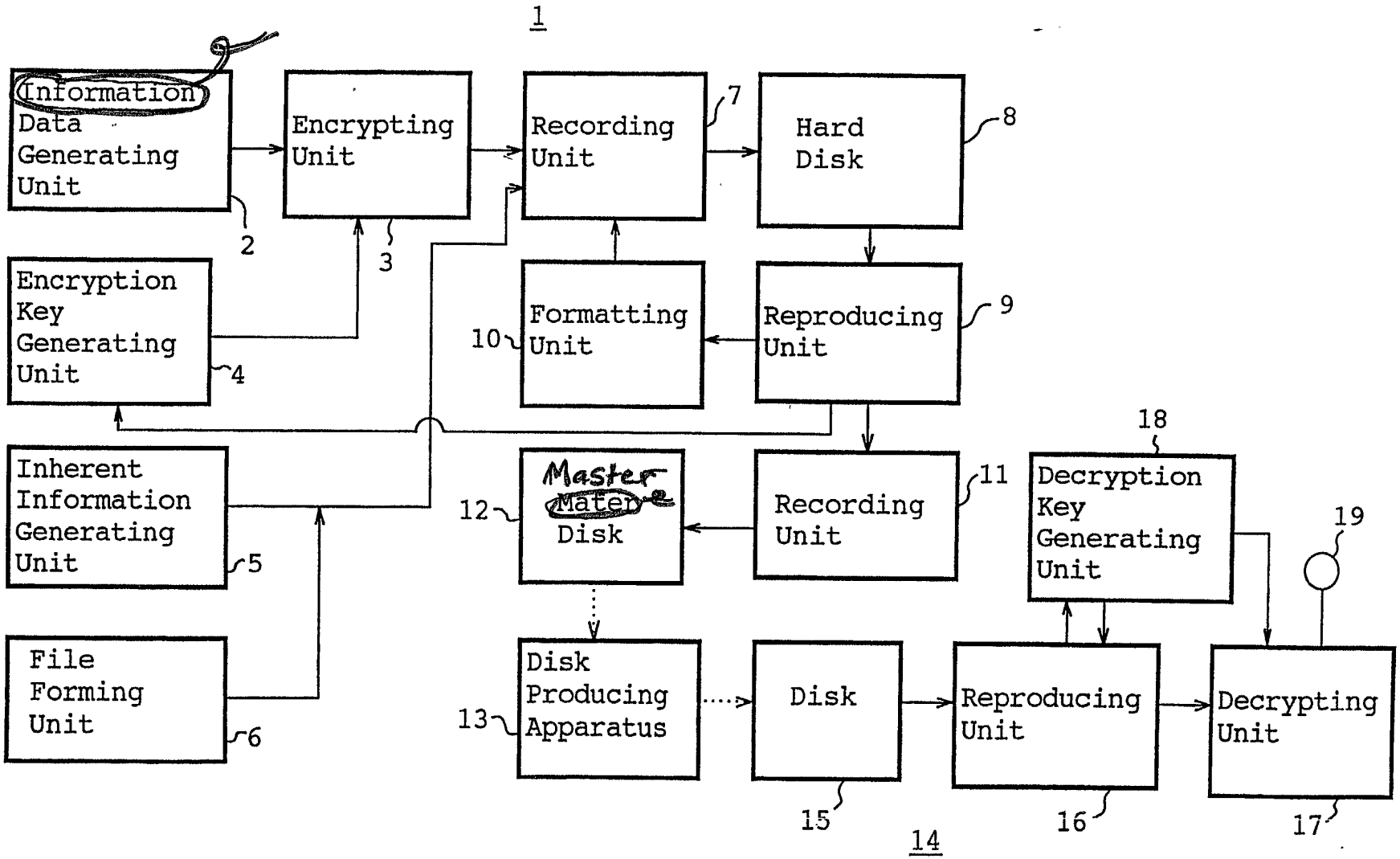

1
Information Data Generating Unit
2
Encrypting Unit
3
Recording Unit
7
Hard Disk
8
Encryption Key Generating Unit
4
Formatting Unit
10
Reproducing Unit
9
Inherent Information Generating Unit
5
Master Material Disk
12
Recording Unit
11
18
Decryption Key Generating Unit
19
File Forming Unit
6
Disk Producing Apparatus
13
Disk
15
Reproducing Unit
16
Decrypting Unit
17
14

FIG. 3

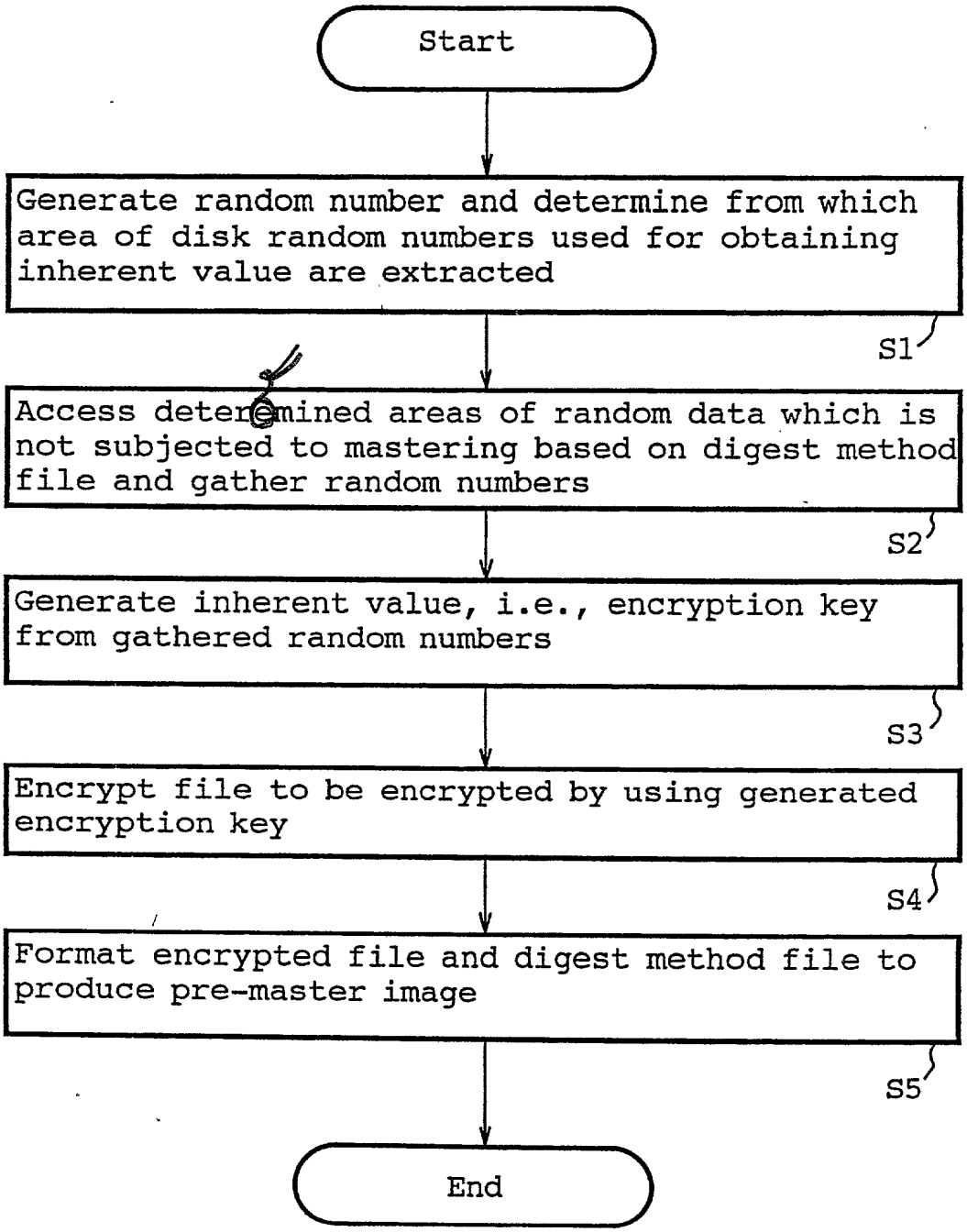

Start
Generate random number and determine from which area of disk random numbers used for obtaining inherent value are extracted
S1
Access determined areas of random data which is not subjected to mastering based on digest method file and gather random numbers
S2
Generate inherent value, i.e., encryption key from gathered random numbers
S3
Encrypt file to be encrypted by using generated encryption key
S4
Format encrypted file and digest method file to produce pre-master image
S5
End

FIG. 6

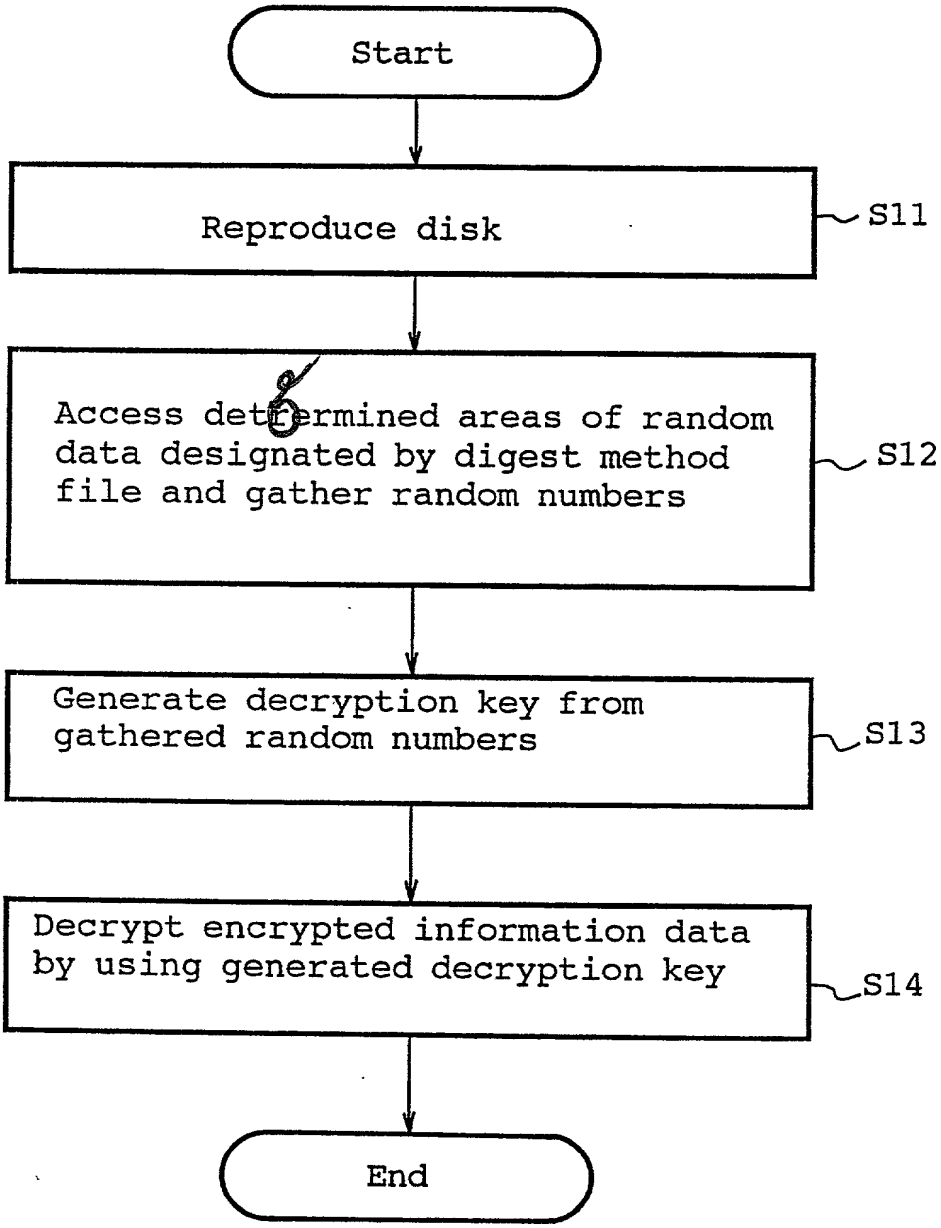

Start
Reproduce disk
S11
Access determined areas of random data designated by digest method file and gather random numbers
S12
Generate decryption key from gathered random numbers
S13
Decrypt encrypted information data by using generated decryption key
S14
End

FIG. 7

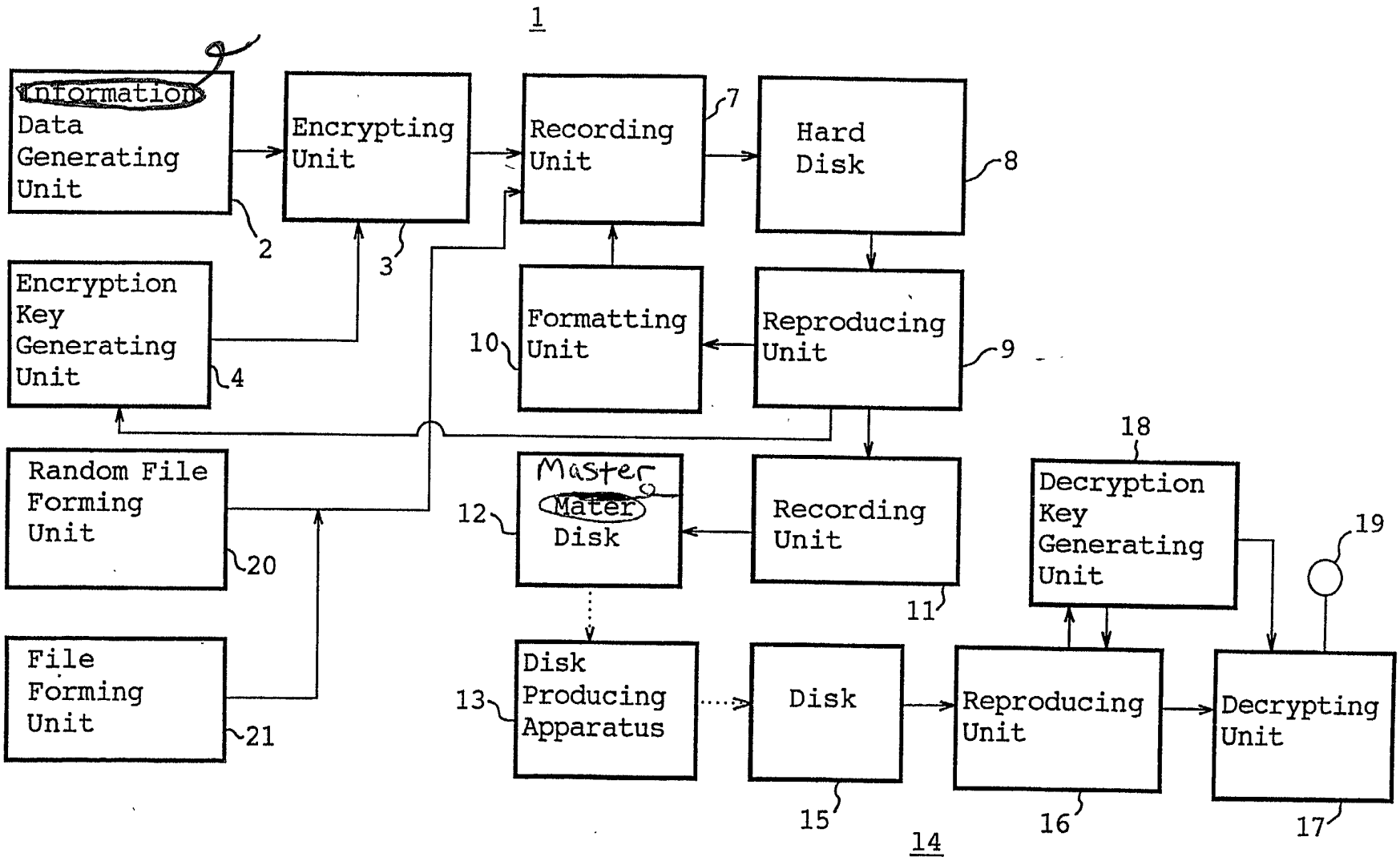

1
Information Data Generating Unit
2
Encrypting Unit
3
Recording Unit
7
Hard Disk
8
Encryption Key Generating Unit
4
Formatting Unit
10
Reproducing Unit
9
Random File Forming Unit
20
Master Mater Disk
12
Recording Unit
11
18
Decryption Key Generating Unit
19
File Forming Unit
21
Disk Producing Apparatus
13
Disk
15
Reproducing Unit
16
Decrypting Unit
17
14

FIG. 9

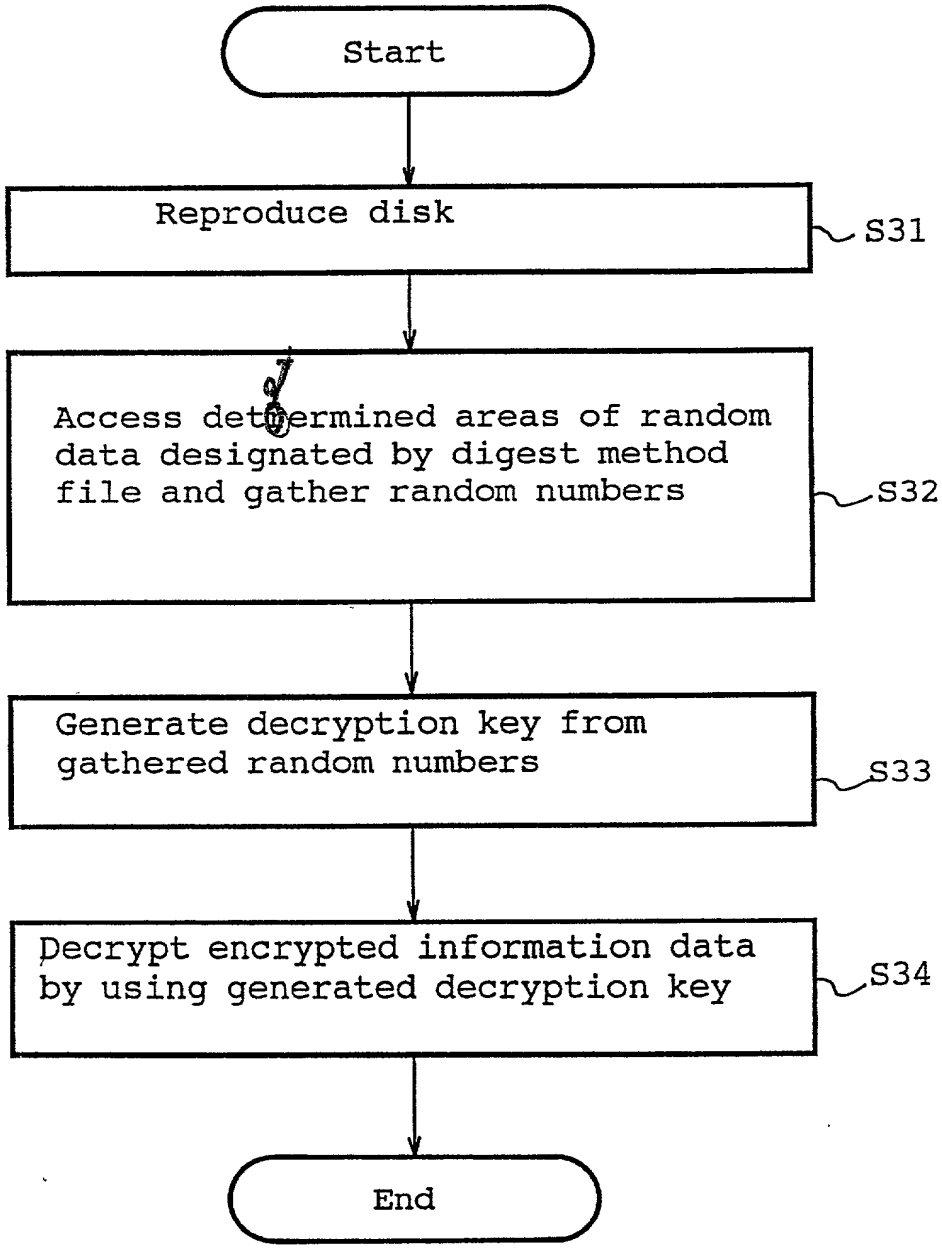

Start
Reproduce disk
S31
Access determined areas of random data designated by digest method file and gather random numbers
S32
Generate decryption key from gathered random numbers
S33
Decrypt encrypted information data by using generated decryption key
S34
End

FIG. 10

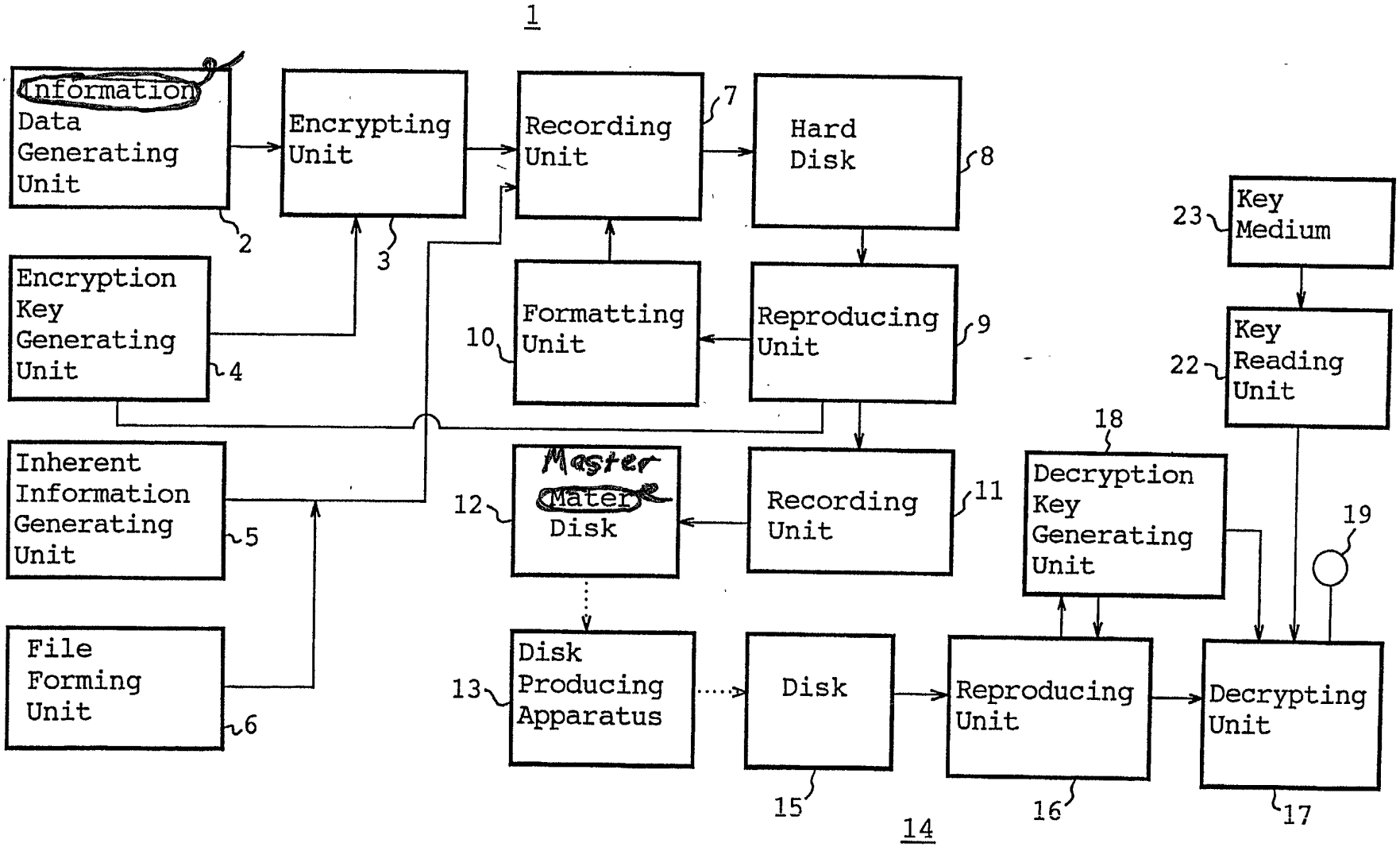

1
Information Data Generating Unit
2
Encrypting Unit
3
Recording Unit
7
Hard Disk
8
Key Medium
23
Encryption Key Generating Unit
4
Formatting Unit
10
Reproducing Unit
9
Key Reading Unit
22
18
Inherent Information Generating Unit
5
Master Mater Disk
12
Recording Unit
11
Decryption Key Generating Unit
19
File Forming Unit
6
Disk Producing Apparatus
13
Disk
15
Reproducing Unit
16
Decrypting Unit
17
14

FIG. 11

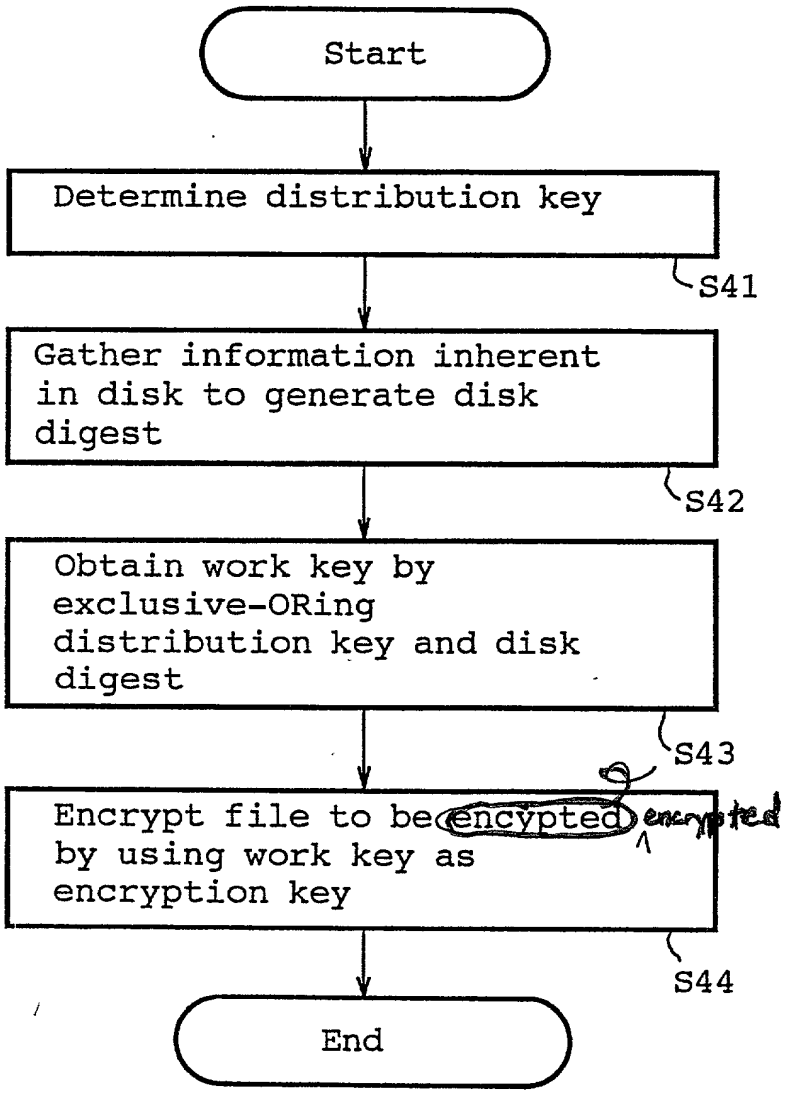

Start
Determine distribution key
S41
Gather information inherent in disk to generate disk digest
S42
Obtain work key by exclusive-ORing distribution key and disk digest
S43
Encrypt file to be encypted by using work key as encryption key
encrypted
S44
End

FIG. 12

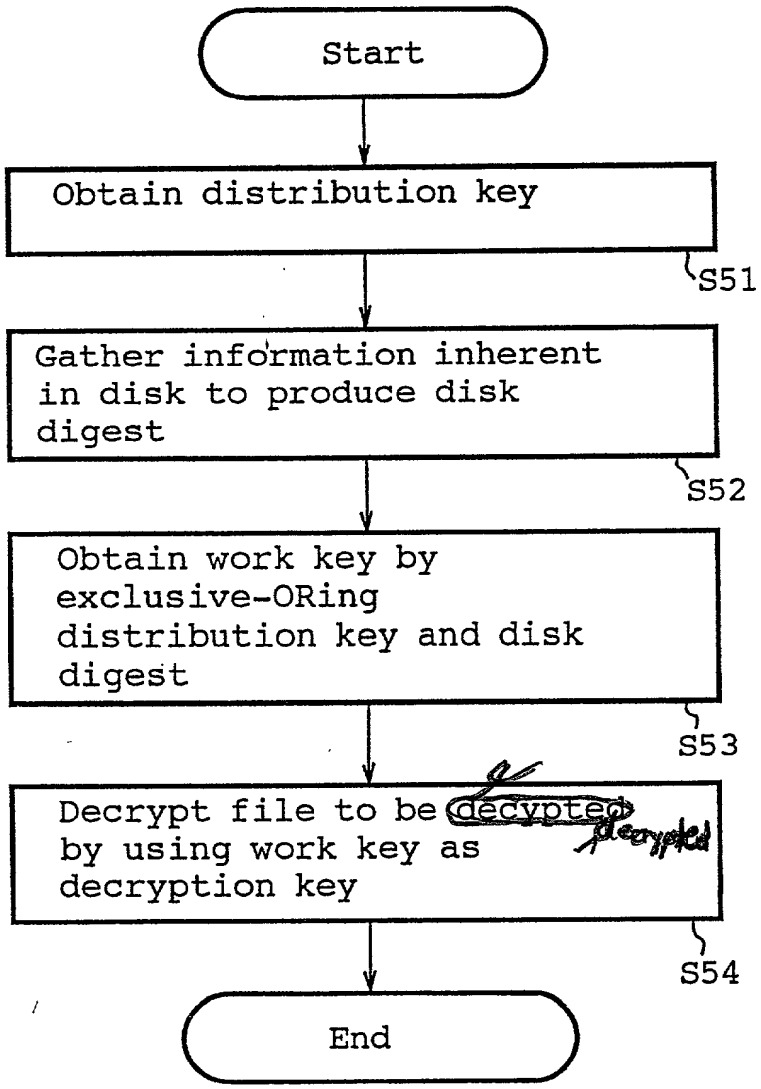
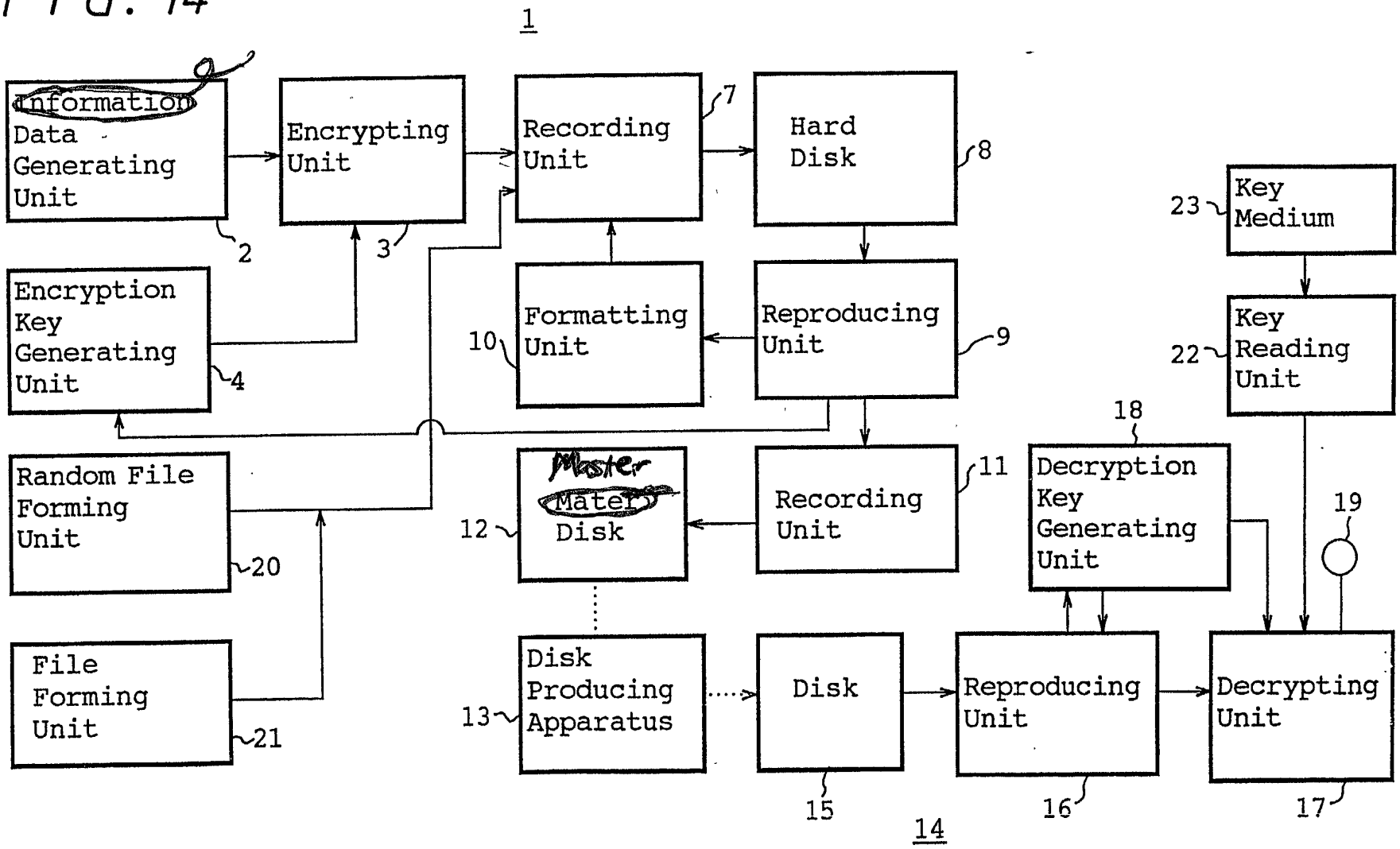

Start
Obtain distribution key
S51
Gather information inherent in disk to produce disk digest
S52
Obtain work key by exclusive-ORing distribution key and disk digest
S53
Decrypt file to be decypted by using work key as decryption key
S54
End

FIG. 14


1
Information Data Generating Unit
2
Encrypting Unit
3
Recording Unit
7
Hard Disk
8
Key Medium
23
Key Reading Unit
22
Encryption Key Generating Unit
4
Formatting Unit
10
Reproducing Unit
9
18
Random File Forming Unit
20
Master Disk
12
Recording Unit
11
Decryption Key Generating Unit
19
File Forming Unit
21
Disk Producing Apparatus
13
Disk
15
Reproducing Unit
16
Decrypting Unit
17
14

DECLARATION FOR PATENT APPLICATION (JOINT OR SOLE)
(Under 37 CFR § 1.63; with Power of Attorney)
FROMMER LAWRENCE & HAUG LLP

FLH File No. 450100-3689

As a below named inventor, I hereby declare that:
My residence, post office address and citizenship are as stated below next to my name,
I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention ENTITLED:

ENCRYPTING METHOD AND APPARATUS, RECORDING METHOD, DECRYPTING METHOD AND APPARATUS, AND RECORDING MEDIUM

the specification of which

____ is attached hereto.

__X__ was filed on October 15, 1996 as Application Serial No. 08/721,310 ,

with amendment(s) through _____ (if applicable, give dates).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.
I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Sec. 1.56.
I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s) [list additional applications on separate page]:

Number:	Country:	Filed (Day/Month/Year):	Priority Claimed: Yes	No
7-267252	Japan	16 October 1995	X	
8-095004	Japan	17 April 1996		X

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code § 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Sec. 1.56, which became available between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U.S. Application(s) [list additional applications on separate page]:

Appln. Ser. Number:	Filed (Day/Month/Year):	Status (patented, pending, abandoned):

I hereby appoint WILLIAM S. FROMMER , Registration No. 25,506 , and DENNIS M. SMID , Registration No. 34,930 or their duly appointed associate, my attorneys, with full power of substitution and revocation, to prosecute this application, to make alterations and amendments therein, to file continuation and divisional applications thereof, to receive the Patent, and to transact all business in the Patent and Trademark Office and in the Courts in connection therewith, and specify that all communications about the application are to be directed to the following correspondence address:

WILLIAM S. FROMMER , Esq.
c/o FROMMER LAWRENCE & HAUG LLP
745 Fifth Avenue
New York, New York 10151

Direct all telephone calls to:
(212) 588-0800
to the attention of:
WILLIAM S. FROMMER

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

INVENTOR(S):
Signature: Ryuji Ishiguro Date: Jan. 8, 1999
Full name of sole or first inventor: Ryuji ISHIGURO
Residence: Tokyo, Japan
Citizenship: Japan

Signature: Masafumi Minami Date: Jan. 8, 1999
Full name of 2nd joint inventor (if any): Masafumi MINAMI
Residence: Tokyo, Japan
Citizenship: Japan

Signature: _____ Date: _____
Full name of 3rd joint inventor (if any):
Residence:
Citizenship:

[Similarly list additional inventors on separate page]
Post Office Address(es) of inventor(s):
[if all inventors have the same post office address]

Sony Corporation
7-35 Kitashinagawa 6-chome
Shinagawa-Ku, Tokyo 141, Japan

Note: In order to qualify for reduced fees available to Small Entities, each inventor and any other individual or entity having rights to the invention must also sign an appropriate separate "Verified Statement (Declaration) Claiming [or Supporting a Claim by Another for] Small Entity Status" form [e.g. for Independent Inventor, Small Business Concern, Nonprofit Organization, individual Non-Inventor].
Note: A post office address must be provided for each inventor.